Office of Technology Assessment

Congressional Board of the 100th Congress

MORRIS K. UDALL, *Arizona, Chairman*

TED STEVENS, *Alaska, Vice Chairman*

Senate

ORRIN G. HATCH
Utah

CHARLES E. GRASSLEY
Iowa

EDWARD M. KENNEDY
Massachusetts

ERNEST F. HOLLINGS
South Carolina

CLAIBORNE PELL
Rhode Island

House

GEORGE E. BROWN, JR.
California

JOHN D. DINGELL
Michigan

CLARENCE E. MILLER
Ohio

DON SUNDQUIST
Tennessee

AMO HOUGHTON
New York

JOHN H. GIBBONS
(Nonvoting)

Advisory Council

WILLIAM J. PERRY, *Chairman*
H&Q Technology Partners

DAVID S. POTTER, *Vice Chairman*
General Motors Corp. (Ret.)

EARL BEISTLINE
Consultant

CHARLES A. BOWSHER
General Accounting Office

CLAIRE T. DEDRICK
California Land Commission

S. DAVID FREEMAN
Lower Colorado River Authority

MICHEL T. HALBOUTY
Michel T. Halbouty Energy Co.

CARL N. HODGES
University of Arizona

RACHEL McCULLOCH
Brandeis University

CHASE N. PETERSON
University of Utah

JOSEPH E. ROSS
Congressional Research Service

Director

JOHN H. GIBBONS

The Technology Assessment Board approves the release of this report. The views expressed in this report are not necessarily those of the Board, OTA Advisory Council, or individual members thereof.

SCIENCE TECHNOLOGY AND THE FIRST AMENDMENT

SPECIAL REPORT

CONGRESS OF THE UNITED STATES
Office of Technology Assessment
Washington, DC 20510-8025

J952-4

Recommended Citation:

U.S. Congress, Office of Technology Assessment, *Science, Technology, and the First Amendment*, OTA-CIT-369 (Washington, DC: U.S. Government Printing Office, January 1988).

Library of Congress Catalog Card Number 87-619897

For sale by the Superintendent of Documents
U.S. Government Printing Office, Washington, DC 20402-9325
(order form can be found in the back of this report)

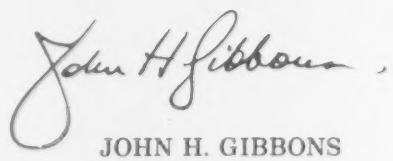
Foreword

In honor of the Bicentennial of the United States Constitution, OTA is conducting a study of *Science, Technology, and the Constitution.* At the request of the Committee on the Judiciary of the House of Representatives, and its Subcommittee on Courts, Civil Liberties, and the Administration of Justice, we are examining ways in which continuing scientific advances and new technological developments may influence the scope and meaning of enduring constitutional principles and protections. A background paper, *Science, Technology, and the Constitution*, was released in September 1987.

Freedom of speech and press, embodied in the First Amendment, are among the most cherished of those protections. As the first of a series of special reports this document considers challenges to freedom of speech and press that come from the advance of science and technology.

Part I of the report discusses how the meaning of "the press" has expanded from printed material to include a wide range of broadcast and electronic media. Satellites, computers, electronic bulletin boards, teletex, videotext, and other new ways of gathering, editing, and delivering news are blurring legal and regulatory distinctions between common carriers and "the press," thus changing arguments about the constitutional rights that they have each enjoyed.

Part II addresses freedom of speech and press as they apply to scientific communications and technological know-how. As science and technology become ever more important to our economy and our military strength, the delicate balance between individual rights and the national interest becomes both more important and more difficult to maintain.



JOHN H. GIBBONS
Director

Science, Technology, and the First Amendment
OTA Project Staff

John Andelin, *Assistant Director, OTA*
Science, Information, and Natural Resources Division

Fred W. Weingarten, *Program Manager*
Communication and Information Technologies Program

Program Staff

Vary T. Coates, *Project Director*

Benjamin C. Amick III, *Analyst**

Robert Kost, *Analyst*

Mary Ann Madison, *Research Analyst*

Administrative Staff

Liz Emanuel Sandra Holland Becky Battle

*Until May 1987.

Contents

Page

Summary 1

Part I. Freedom of the Press in the Information Age

Chapter 1. New Technologies for Gathering News and Information 5
- Newsgathering 9
- Computer Databases 10
- Media Satellites 11
- Implications for Privacy 12
- Implications for National Security 16

Chapter 2. New Technologies for Editing and Selecting News and Information 19
- Electronic Publishing 19
- Editorial Control and Liability 21
- Global Networks and the International Press 23

Chapter 3. New Technologies for Publishing and Disseminating News and Information 27
- The Convergence of the Media 27
- Cable Television 30
- Information Services Delivered Over Telephone Lines 32

Part II. Scientific Communications and the First Amendment

Chapter 4. National Security and Scientific Communications 37
- Science, Free Speech, and National Security 37
- The Executive Branch and Classification of Documents 41
- Export Controls 49

Chapter 5. The 1980s: Converging Restrictions on Scientific Communications 55
- Contractual Restrictions on Communications 55
- Restrictions on Informal Communications 56
- Self-Restraint 59
- National Security Directives and the Role of the National Security Agency 60

Chapter 6. Constitutional Issues: An Overview 65

Appendix A. Acknowledgments 71

Summary

The First Amendment says:

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for redress of grievances.

The provisions of the First Amendment are designed to protect the most sensitive areas of personal belief—religion, ethics, political philosophy—and to act as a bulwark against government intervention in the most basic elements of our democracy: the expression of thought and opinion. As necessary conditions to democratic governance, the rights embodied in the First Amendment occupy a "preferred position" in the hierarchy of constitutional rights and powers. The first clear statement of this preferred position doctrine came in *Thomas v. Collins*, in which Justice Rutledge, speaking for the majority of the Supreme Court, said:

> This case confronts us again with the duty our system places on this Court to say where the individual's freedom ends and the State's power begins. Choice on that border, now as always delicate, is perhaps more so where the usual presumption supporting legislation is balanced by the preferred place given in our scheme to the great, the indispensable democratic freedoms secured by the First Amendment . . . That priority gives these liberties a sanctity and a sanction not permitting dubious intrusions, and it is the character of the right, not of the limitation, which determines what standard governs the choice . . . .[1]

Notwithstanding the absolute language of the First Amendment and its preferred position in the constitutional order, however, the Supreme Court has never interpreted freedoms of religion, speech, press, or assembly to be without limitation. These rights, which are collectively referred to as freedom of expression, can be limited in a variety of ways. Government can prohibit entirely speech that is obscene, threatens national security, or is an incitement to imminent violence or to the overthrow of the government; it can place reasonable restrictions as to the time, place, and manner of commercial speech or speech that takes place in public; it can force one to compensate victims of defamation and other forms of speech injurious to private interests; and it can regulate speech that takes place over the airwaves. Moreover, when speech or the exercise of religion merges into action, government can regulate those forms of expression to protect the public health, safety, and welfare.

As necessary conditions to democratic governance, the rights embodied in the First Amendment occupy a "preferred position."

Because freedom of expression is not absolute, it often involves a balancing of governmental interests against the rights of individuals where the two are in conflict. Balancing rights against power occurs in the context of contemporary values and institutions: economic, political, ethical, legal, and scientific or technological.

Science and technology may affect the balance between First Amendment rights and government interest by changing power relationships.

Science and technology may affect the balance between First Amendment rights and government interest by changing power relationships between individuals and between the individual and the state. As it first did with the printing press, technology will give rise to new ways of communicating, which amplify the ways in which individuals and organizations express themselves. Information and communications technologies, such as satel-

[1] 323 U.S. 516, 530 (1945).

lites, computers, and digital transmission lines, are, like the telegraph, telephone, radio, and television technologies before them, changing the ways in which we communicate ideas, theories, opinions, and incitements to action—they affect who can say what, to whom, to how many, and at what cost.

Taken together, advances in computers and telecommunications may change the concept of "the press" from one in which one organization publishes for many to one in which many share information amongst themselves. With these changes will come new First Amendment challenges to the power of the government to regulate access to and ownership of communications media. New technologies, such as electronic publishing, may not fit easily into old models of regulation, and First Amendment distinctions between the rights of print publishers, broadcasters, and common carriers will become increasingly difficult to justify.

Distinctions between the First Amendment rights of print publishers, broadcasters, and common carriers will become increasingly difficult to justify.

New capabilities for the press to gather, store, and retrieve information on individuals may require that rules of liability for constitutionally protected speech be reexamined. The potential for technology to decentralize the editorial function may raise questions of editorial control and liability under the First Amendment. And, in an era of global communications, the question of whether First Amendment rights extend to foreign speakers in this country, or to speakers in foreign countries when they are heard or read here, will also be raised.

The open communication of scientific information—data, hypotheses, conclusions, explanatory theories, technological know-how—is a special kind of speech or publication. There is no consensus on the question as to whether scientific communication enjoys the full protection provided by the First Amendment to political communications. In a society in which science and technology play a central and critical role, this is an issue meriting continuing attention and debate.

It is well established that scientific communication can be limited when necessary to protect national security. But how severe can and should that limitation be? As science and technology become ever more important to our economy and our military strength, the delicate balance between individual rights and the national interest becomes both more important and more difficult to maintain. Do the limits imposed by classification, congressionally legislated restrictions, and export controls, collectively negate the right of free speech and free press in the field of science?

In fields such as mathematics, biology, or physics, basic research results in certain areas can have direct and immediate implications for technological development. In those cases, where the line between basic knowledge (science) and its implementation (technology) becomes thin and difficult to discern, a balance between the right of expression and interests of the state in preserving security is very difficult to achieve. There are likely to be many situations in the future in which the government will assert compelling reasons for limiting basic scientific communications.

Part I

Freedom of the Press in the Information Age

We should note the force, effect, and consequences of inventions which are nowhere more conspicuous than those three which were unknown to the ancients, namely, printing, gunpowder, and the compass. For these three have changed the appearance and state of the whole world . . .

—Francis Bacon, Novum Organum, Aphorism 129*

Networked computers will be the printing presses of the twenty-first century. If they are not free of public control, the continued application of constitutional immunities to the nonelectronic [press] . . . may become no more than a quaint archaism, a sort of Hyde Park Corner where a few eccentrics can gather while the major policy debates take place elsewhere.

—Ithiel de Sola Pool, *Technologies of Freedom* (1983)

*As quoted in Elizabeth L. Eisenstein, *Printing Press as an Agent of Change* (Cambridge, MA: Cambridge University Press, 1979), vol. 1, p. 43.

Chapter 1

New Technologies for Gathering News and Information

Despite its origins in the context of printing, "freedom of the press" has come to be interpreted as protecting communication to the public generally, regardless of the medium. Print media, motion pictures, broadcasting, cable television, and even the mails have come to be considered as the "press" for purposes of the First Amendment. As the Supreme Court has said, "[press] comprehends every sort of publication which affords a vehicle of information and opinion."[1] Moreover, while some have argued that freedom of the press was only intended to shield the dissemination of news and opinion, the protections of the First Amendment have been extended to protect scientific, literary, and artistic messages as well. It is this broad notion of the press as a vehicle for every kind of public expression that is used in this report.

The printing press provided, for the first time, a capability for mass communication, whereby one individual or organization could inform, entertain, or persuade many others. At the time the Constitution was written, publishing in the United States had not yet become the "mass medium" it is today.[2] A craftsman printer produced one page at a time, and could produce about 2000 copies of it in a 10-hour day. The technology was inherently egalitarian; it took neither political power nor large sums of money for an individual to publish a work. The "freedom of the press" had a more or less literal meaning; government was prohibited from licensing or otherwise controlling the use of the technology.[3]

In the two centuries that have passed since the ratification of the First Amendment, innovations in technology have added to the variety and power of the press, and have, as a consequence, changed the social, economic, and political impact that the press has had.[4] Thanks in large measure to technologies such as the communications satellite, for example, global television is now a reality; over 500 million people watched the moon landing in 1969, and over 2 billion may have seen the Los Angeles Olympics in 1984.[5]

Changes to the legal environment in which the press operates have accompanied these technological changes.[6] "Freedom of the

[1] *Lovell v. Griffin*, 303 U.S. 444, 452 (1938).

[2] The press as a mass medium awaited the industrial revolution; with its steam-driven power (and later rotary) presses, which increased production tenfold, and its new modes of distribution, its assembly line methods, and division of entrepreneurial functions. Ithiel de Sola Pool, *Technologies of Freedom* (Cambridge, MA: Belknap Press, 1983). (Hereafter referred to as *Technologies of Freedom*) and *Encyclopedia Britannica*, "Publishing," 1986.

[3] The importance of this concept must be understood in the context of the English law that preceded it, which granted the Stationers Company monopoly rights over printing and required government licensing to own and operate a printing press. Even after the ratification of the First Amendment in America in 1791, however, the exercise of this freedom could be severely curtailed and punished.

[4] The new capability for rapid, accurate, and mass publication provided by the printing press facilitated the speed with which the Protestant Reformation spread through Europe: "heralded on all sides as a 'peaceful art,' Gutenberg's invention probably contributed more to destroying Christian concord and inflaming religious warfare than any of the so-called arts of war ever did." *Printing Press as an Agent of Change* (Cambridge, MA: Cambridge University Press, 1979), p. 319. Four centuries later, with live coverage of the civil rights movement in the American south, and riots in the north, east, and west, radio and television thrust the issue of racial equality before the American public in the 1960s. Television has also been credited with a major role in ending the United States' involvement in the Vietnam War. Michael Mandelbaum, "Vietnam: The Television War," *Daedalus*, fall 1982, p. 157.

[5] Joseph Pelton, "The Technological Environment," *Toward a Law of Global Communications Networks*, Anne Branscomb (ed.), by the Science and Technology Section of the American Bar Association (New York: Longman, 1986), pp. 37, 43.

[6] The inherent differences in the technology of print and that of broadcast, for example, led the Supreme Court to uphold the FCC's regulation of "indecent" speech over broadcasting, because of broadcasting's "uniquely pervasive presence on the lives of all Americans," and the fact that "prior warnings cannot completely protect the listener or viewer from unexpected program content," *FCC v. Pacifica Foundation*, 438 U.S. 726, reh. denied, 439 U.S. 883 (1978).

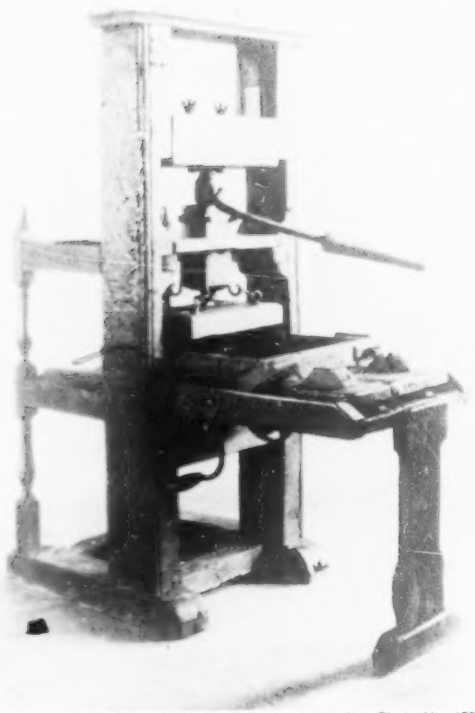


Photo credit: Smithsonian Institution, Photo No. 17539B

Franklin Press

Photo credit: National Aeronautics and Space Administration

Communications satellite SBS-3 being deployed from Space Shuttle Columbia

Today communication satellites distribute staggering amounts of information over thousands of miles in a fraction of the time needed for Ben Franklin's press to print one page.

press" has been extended to all forms of publishing, but real or perceived limitations on the technology—most notably, in the case of broadcasting—have nevertheless resulted in a patchwork of exceptions to the freedoms originally granted the printing press.

However, even broadcasting, with its national and now global audience, and its compelling use of images from all over the world, did not change the "one-to-many" nature of journalism that has characterized the press since the first era of printing. Although the number of broadcast organizations now far exceeds that of newspapers, legal and economic barriers to entering and successfully competing as a broadcaster have perpetuated this one-to-many character.

New technologies will not only augment the capabilities of the press they may give rise to new forms of press, alien to the last 200 years of First Amendment jurisprudence.

Observers argue that we are now entering an era that is variously referred to as an information age, an information society, or a post-industrial economy. These phrases conjure images of new technologies—high-speed computers, global communications networks, "in-

telligent" machines, and low-cost storage media of astonishing capacity. But, more important for present purposes is what these technologies mean for the structure of communications, and consequently, for the way in which the press gathers and publishes information. In changing the way in which information is produced and disseminated, technology may change who and what is considered "the press." New technologies will not only augment the capabilities of the press as we know it today, they may give rise to new forms of press, alien to the last 200 years of First Amendment jurisprudence.

Taken together, current and anticipated advances in technology suggest a fundamental shift from the concept of "press" to the concept of "network." To some extent, the past mode of one organization *publishing* for many may give way to a *communications* mode in which many share knowledge among themselves. One-to-many publication will no doubt continue, but will be joined by new and unfamiliar forms. Gathering, editing, and disseminating news and information, which today is commonly integrated in one organization, may eventually be fragmented between many specialized entities. The electronic publisher of the future may act more as a clearinghouse for the exchange of news and information than as a gatherer. Global electronic networks may eventually allow the gathering, writing, filming, editing, and publishing of news to be decentralized among many organizations, which may sell one another specialized services.

One-to-many publishing will also coexist with one-to-one publishing, such as electronic mail, and many-to-many publishing, such as computer conferencing. Each of these permutations may merge into the other under given circumstances—what started out as an electronic mail message may be integrated into a broadcast, which individuals may then store in a database, to be redistributed in different forms to different audiences. Specialized, individualized reports may be generated by one organization for a few subscribers or patrons, and distributed over electronic mail. Pieces of one message may be integrated into a whole and distributed to an audience larger or smaller than the original.

New forms of publishing will grow up alongside the "mass" communication that we are familiar with today. Individuals will be able to select the subject matter of the information they receive, and determine its format and manner of presentation. This processing may be done by consumers at intelligent terminals in their home or business, or it may be done further "up the line," by the local telephone or cable company.

As a consequence of this shift from a centralized press with a uniform product to a decentralized network selling diverse services, the courts and Congress may face new questions of constitutional interpretation not presented when the press was a more or less distinct, identifiable institution. Even today, with the convergence of information processing with telecommunications, questions of categorization for purposes of the First Amendment—beyond those of common carrier, broadcaster, and print publisher—are emerging.

Like the underground press that flourished in the 1960s, the electronic underground press may become the crucible of cultural change.

Technology will further challenge distinctions between the freedoms of speech and press, "nonmedia" and "media" that were already difficult to make. Whether there is a difference between First Amendment rights of speech and press is a matter of disagreement among scholars,[7] but practical consequences

[7]Scholars disagree over whether the distinction between the freedom of speech and the freedom of the press is of constitutional or legal significance. Former Supreme Court Justice Potter Stewart, for example, adheres to the view that freedom of speech, worship, assembly, and other liberties guaranteed by the Bill of Rights are substantive and individual in nature, while the freedom of the press is "structural," and extends freedom of expression to an institution. "The publishing business is, in short, the only organized private business that is given explicit constitutional protection." Potter Stewart, "Or of the Press,"

flow from it. Many of our 20th century assumptions about freedom of the press depend on notions of the press as a business, located in a community, dependent on the support of readers and viewers, committed to a regular cycle of publication and broadcast, managed by responsible persons, and striving—to some degree—for objectivity, balance, and a fair presentation of the facts. What if those elements change?

The Colonial press was characterized by irregular appearance, pseudonymous invective, and a boisterous lack of respect for any form of government. Modern, high-technology international versions of this may flourish in parallel with the established press. New interactive communications technologies can make producing and disseminating underground "newspapers" as economical as a phone call, and as egalitarian as a New England town meeting. Like the underground press that flourished in the decades before and after the First World War, and again in the 1960s, the electronic underground press may become the crucible of cultural change.[8] The first simple experiments of this sort are already underway on many computer bulletin boards.

New questions of liability and potential for harm will also be raised. Distinctions between primary publishers, secondary publishers, and republishers—which served to allocate responsibility for defamatory publications—will be more difficult to make.[9] Locating the "source" of inaccurate or false information that causes harm may prove elusive on electronic networks. The press' use of remote sensing systems

Limitations on the liberty of the press may come from a failure to reconcile private ownership interests in the physical media with public interest in the message carried over these media.

aboard orbital satellites, or "mediasats," together with an unprecedented ability to search, store, and process large amounts of information on individuals may give rise to new concerns over the ongoing conflict between privacy and freedom of the press.

The continuing debate over the deleterious effects of barriers to entry on the diversity of news and information available, and the role of government in mitigating them, will intensify. The assumption of Classical Liberalism, that the principal threat to individual liberty is from large public organizations—such as the Federal Government—may no longer hold. Instead, limitations on the liberty of the press may come from a failure to reconcile private ownership interests in the physical media with public interest in the message carried over these media.

Courts and First Amendment scholars have developed a variety of ways of classifying and organizing the functions of the press for purposes of analyzing First Amendment issues.[10]

26 *Hastings Law Journal* 631 (1975). Former Chief Justice Burger disagrees, arguing that "the First Amendment does not 'belong' to any definable category of persons or entities: it belongs to all who exercise its freedoms." *First National Bank of Boston v. Bellotti*, 435 U.S. 765, (1978), Burger, J. concurring.

[8]The "cultural revolution" of the 1960s found expression and momentum in a thriving underground press—"[o]nly on the pages of the underground press, with its melange of stories, articles, events, hunches, graphics, fantasies, exposés and theories can one find the Movement." Laurence Learner, *The Paper Revolutionaries: The Rise of the Underground Press* (New York: Simon & Shuster, 1972) p. 14.

[9]W. Keeton, D. Dobbs, R. Keeton, and D. Owen, *Prosser and Keeton on Torts* (St. Paul, MN: West Publishing Company, 1984), pp. 799-811.

[10]For purposes of assessing the press' regulatory status and shielding from liability under the First Amendment, a distinction is commonly made between the press as printed medium, as broadcaster, and as common carriers (which are not considered press). OTA Workshop on "The Future of the Press and the First Amendment," Mar. 26, 1987, Washington, DC. See also: Richard Neustadt, *The Birth of Electronic Publishing* (White Plains, NY: Knowledge Industry Publications, Inc., 1982); and Lynn Becker "Electronic Publishing: First Amendment Issues in the Twenty First Century," 13 *Fordham Urban Law Journal* 801 (1984). With regard to defamation, one textbook organizes constitutional privileges around notions of the press as the originator of speech, as commentator, or as repeater. Marc Franklin, *Cases and Materials on Mass Media Law* (Mineola, NY: Foundation Press, Inc., 1987). In analyzing First Amendment tensions between rights of access and exclusion, another author distinguishes between the press as editor (making decisions about the content of messages, which decisions are protected by the First Amendment) and the press as owner (making decisions about the use of the medium, which decisions are protected by the Fifth Amendment). Mark Nadel, "A Unified Theory of the First Amendment: Divorcing the Medium from the Message," 11 *Fordham Urban Law Journal* 163 (1983).

Familiar constitutional issues—pitting freedom of the press against privacy rights and national security interests—will be placed in unfamiliar contexts.

Because this report is concerned with the impact of technological innovation on the press, however, press functions will be organized along lines that reflect more or less discrete types of capabilities offered by new technologies. These capabilities and press functions can be most usefully grouped as follows:

- New technologies for gathering news and information: databases and satellites
- New technologies for editing news and information: electronic publishing
- New technologies for publishing and disseminating news and information: the convergence of computers and communications.

The rest of this chapter will deal with the first of these broad topics; new technologies for editing and publishing are covered in chapters 2 and 3 respectively.

NEWSGATHERING

In order to publish news and information, the press must have an ability to gather it in the first place. The Supreme Court has yet to decide, however, whether newsgathering is itself a protected First Amendment activity, separate from speaking and publishing.[11] The Supreme Court said in *Branzburg v. Hayes* that "it is not suggested that news gathering does not qualify for First Amendment Protection; without some protection for seeking out the news, freedom of the press could be eviscerated.[12] . . ." However, the Court has declined to say that government has a positive duty to allow journalists special access to information. The press has access to government proceedings, records, or other information that is available to members of the public generally.[13] Presumably, the converse is also true; access denied to the general public may also be denied to the press,[14] but the government may not close down avenues for gathering and acquiring news that *are* generally available to the public, without a compelling reason.

Mediasat would supply a stream of timely information—peering where repressive governments or dangerous natural environments had formerly kept the press at bay.

Although the press may not, as a constitutional matter, have any greater *rights* to gather information than the general public, they may, as a practical matter, have a greater and more concerted *ability* to gather information than most individuals. In the coming years, technology will greatly amplify the information-gathering resources of the press. As a result, familiar constitutional issues—pitting freedom of the press against privacy rights and national security interests—will be placed in unfamiliar contexts. Technology is likely to blur distinctions between gathering information and publishing it, and the Court will eventually have to confront the question of whether the press'

[11] *Branzburg v. Hayes*, 408 U.S. 665 (1972)
[12] Ibid., p. 681.
[13] *Pell v. Procunier*, 417 U.S. 817 (1974); *Saxbe v. Washington Post Co.*, 417 U.S. 843 (1974); cf., *Houchins v. KQED*, 438 U.S. 1 (1978). See also, Rita Ann Reimer, *Legal and Constitutional Issues Involved in Mediasat Activities* (Washington, DC: Congressional Research Service, The Library of Congress, 1987), Report No. 86-823A, pp. 6-8.
[14] When, in 1983, the United States invaded Grenada, the government imposed a total news blackout and prohibited members of the public and the press from traveling to Grenada. The press sought prospectively to enjoin the Executive from imposing any such future ban. The case was dismissed as moot, but the court went on to say that "[the] decision whether or not to impose a press ban during military operations and the nature and extent of such a ban if imposed are matters that necessarily must be left to the discretion of the commander in the field." *Flynt v. Weinberger*, 588 F.Supp. 57, 61 (D.D.C. 1984), affirmed (on the basis of mootness), 762 F.2d 134 (D.C. Cir. 1985).

interests in gathering news merit constitutional protection under the First Amendment. Among the new tools that the press will have at its disposal for gathering information are computer databases and remote sensing satellites. The use of these technologies may raise a number of constitutional questions concerning, for example, individual privacy rights, national security, and the expungement of records.

COMPUTER DATABASES

Databases are records of information stored in machine readable form, and are typically accessible by personal computer over packet-switched data networks (e.g., Telenet, Tymnet, or a variety of privately owned communications networks). Information in electronic databases is usually searched and retrieved by software provided by the vendor of the database service.

For purposes of this report, the concept of computer databases is kept separate from that of electronic publishing, which is discussed in chapter 3. In reality, database vendors are, by definition, also electronic publishers, since they publish information in an electronic, machine-readable form. However, electronic publishing is a broader concept, which includes transactional services (i.e., banking and merchandising) and messaging services that are beyond those available from database vendors. Perhaps the distinction is easiest to make in the following way: database vendors provide information; electronic publishers provide information *services*, which may include database access.[15]

The database industry is growing at a rate of 15 to 18 percent a year. Total revenues were estimated to be $2.2 billion in 1986, and are projected to be more than $4.2 billion by 1990.[16] In 1986, there were 3,200 online database services available worldwide compared with 400 in 1979.[17]

In principle, anything that can be represented in digital form can be stored and retrieved from a database. Today, this includes the full text of newspapers, magazines, journals, and publications from any major scientific or professional discipline. In the future, computer software, motion or still pictures, and high fidelity music and voice will be stored on computer and shipped over telephone or cable television lines. Existing database services are categorized as bibliographic and abstractive (e.g. the Library of Congress' SCORPIO); full text (e.g. Mead Data Central's LEXIS); or numeric (e.g. Data Resources, Inc.'s DRI-Securities and Exchange, Current Economic Indicators, Bank Analysis Service, and Financial and Credit Statistics).[18]

Optical disk storage (principally, Compact Disk Read-Only-Memory, or CD-ROM), with its extremely high capacity, low cost, and durability, is likely to change both the economics of online databases, and the type of information sought on them. Optical disks offer much more powerful searching software, and avoid rising telecommunications costs. In the future,

[15]Terminology for these new forms of publishing is still unsettled. In the "Huber Report," the author distinguishes between "*information service providers*," who offer call and network management services, time-shared computing, access and retrieval systems, messaging systems, and transactional services, and "*computerized databases and electronic publishers*," who offer retrieval of documents, data and text from magnetic or other storage media. *The Geodesic Network: 1987 Report on Competition in the Telephone Industry*, prepared by Peter Huber as a consultant to the Department of Justice, Antitrust Division, January 1987, chs. 6 and 7. Other authors make the distinction between *online databases* and *videotex*. See, e.g., Hugh E. Look, *Electronic Publishing—A Snapshot of the Early 1980s* (Oxford, England: Learned Information, 1983).

[16]*Online Database Systems Market in the U.S.* (#1517), Frost and Sullivan, Inc. 1986, as quoted in *Information Hotline* vol. 19, No. 2, February 1987, p. 3.

[17]From Information Industry Association estimates.

[18]This taxonomy was put forth by Martha Williams, "Electronic Databases," *Science*, vol. 228, Apr. 26, 1985, pp. 445-456.

news organizations might make extensive use of optical disks instead of the online services employed in the past.[19]

Today, there are many "gateway" services, in which one database vendor sells the information services of another. A possible scenario for the future database industry is the emergence of a "meta-library" or "virtual database," which would interconnect many or all of the now separate database services. Such a system might allow a user to enter a query in everyday English on any given subject, conduct a search for the location of the information, and retrieve it. Achieving this goal depends on, among other things, considerable technical progress on computer memory, transmission, and processing speeds; advances in computer software; and the development of standards controlling how computers and networks "talk" to one another. Current technological trends suggest that this scenario is obtainable.[20] Much depends on the establishment of standards.[21]

Databases—whether online or on disk—are powerful tools for the press. Researching stories, investigating the background of subjects and sources, corroborating information, drawing out latent connections between people and events, and constructing "mosaics" of information from disparate sources, will all become more practicable, and in some cases, possible for the first time.

It is safe to say that, by the end of this decade, every recent news story, news picture, wire service report, and major press release will be commercially searchable from the reporter's workstation, subject only to the cost his newspaper is willing to incur. The press will have a long and comprehensive memory.

[19]*Optical/Electronic Publishing Directory 1986*, Learned Information. Online databases are likely to remain valuable for time-sensitive, transient information, while CD-ROM will be favored for archival information. See also, Bradford Dixon, "The Impact of CD-ROM on On-Line Data Bases," *CD-ROM Review*, vol. 1, October 1986, p. 52.

[20]Great progress is being made in the ability to transmit large quantities of information very rapidly. INTELSAT satellites can now transmit the equivalent of 20 copies of the *Encyclopedia Britannica* every minute. J. Pelton, M. Perras, and A. Sinha, *INTELSAT, The Global Telecommunications Network* (Honolulu, HI: Pacific Telecommunications Conference, 1983), p. 17. Depending on bandwith required, fiber optic communication cables can now transmit the entire contents of a CD-ROM disk—the equivalent of 200,000 pages of text—in about 1 second. *Science and Technology in Japan*, October-December 1986, p. 8.

[21]These standards concern the way in which information and instructions are communicated to and within a network. The FCC, in its Computer Inquiry III, Phase I Decision, mandated the adoption of an "Open Network Architecture" standard, with the goal of facilitating a total free market in telecommunications and information services. See: A.M. Rutkowski, "Open Network Architectures: An Introduction," *Telecommunications*, February 1987, p. 29. Voluntary communications standards, called Open Systems Interconnect, have already been established by the International Standards Organization.

MEDIA SATELLITES[22]

The news media are increasing the use of satellite imagery in reporting world events. This leads some to believe that the press will soon wish to own and operate their own remote sensing systems dedicated to newsgathering—

[22]The issues concerning media satellites are examined in depth in U.S. Congress, Office of Technology Assessment, *Commercial Newsgathering From Space—A Technical Memorandum*, OTA-TM-ISC-40 (Washington, DC: United States Government Printing Office, May 1987). This section draws solely on the analysis of that publication, hereafter referred to as *Newsgathering from Space*.

termed "mediasat." Mediasat would supply a stream of timely information—peering where repressive governments or dangerous natural environments had formerly kept the press at bay.

Many nations will have their own remote sensing systems within a decade, and the press might purchase data from, or invest in, these foreign systems.

Today's press obtains data from two remote sensing systems, EOSAT—formerly the U.S. Government's Landsat system—and SPOT, a French system.[23] Neither of these systems, however, is particularly well suited to the needs of the press; the resolution of these sensors may be too low (EOSAT yields a maximum of 30 meters resolution, and SPOT a maximum of 10)[24] and their coverage of a given point on the Earth too infrequent for them to be a timely, valuable, and reliable source of information for the press. In addition, the press' access to data cannot be assured because the satellites' owners currently depend on ground stations owned by other countries to collect certain data. It is likely, therefore, that the press would require a dedicated mediasat system to meet their needs.

[23]EOSAT (Earth Observation Satellite Co.) is a private company which now handles the operation and marketing of data for Landsat, which was formerly owned by NASA. For a history of the transfer of the Landsat system to the private sector, see: U.S. Congress, Office of Technology Assessment, *Remote Sensing and the Private Sector: Issues for Discussion—A Technical Memorandum*, OTA-TM-ISC-20 (Springfield, VA: National Technical Information Service, March 1984). SPOT (System Probatoire d'Observation de le Terre) is a French company responsible for marketing the data from the satellite owned by the Government of France.

[24]The greater the resolution of the sensing system, the more detail that can be discerned. The SPOT system, for example, allows one to see individual buildings and highways.

To be effective, a mediasat would need more than high resolution; it must also be able to sense news wherever and whenever it occurs and to transmit the news rapidly to the news agency. A mediasat system would need at least two satellites to ensure same day coverage of events around the globe. In order to receive data in near-real-time, a mediasat system would need to have access to ground stations all over the earth and use on-board tape recorders.

Satellite and database technologies may change the very meaning of "public" and "private."

Although the technology is available to create such a system, including very high resolution technology, the high cost and currently low demand for remotely sensed data will limit media efforts to own and operate a dedicated remote sensing satellite system. Moreover, the value of satellite imagery to the press is uncertain, and is likely to remain so until experience and a more robust remote sensing market combine to define a stable demand for these data. Preliminary calculations indicate that the costs of a mediasat system might exceed its expected revenues.

Notwithstanding the considerable barriers to implementing a mediasat system, it may at some point in the future become a viable concept. The press might form a consortium to share the cost of a mediasat system, or it might resell the data collected by mediasat to subsidize its own use, or it may wait until technical advances reduce the cost of sensors, satellites, and launch vehicles. Moreover, many nations will have their own remote sensing systems within a decade, and the press might purchase data from, or invest in, these foreign systems.

IMPLICATIONS FOR PRIVACY

When the press gathers and publishes information about a person, or uses such information as source material, there is a potential for conflict between the individual's common law

right of privacy and the right of the press to gather and publish news and information. Databases store many pieces of personal information, and permit the creation of larger mosaic pictures of the individual from these pieces. Satellites allow information to be obtained without individuals' knowledge, and without physical intrusion or proximity. Because of the way in which these technologies enhance the newsgathering ability of the press, they create a potential for conflict between privacy and the First Amendment.

Until recently one of the best barricades against breach of privacy was the difficulty and impracticability of integrating all of the public data about a person.

It was in fact the press, and reactions to the press, that first precipitated legal recognition of an individual right to privacy.[25] Privacy is a word that embraces a number of separate but similar values. It has been variously defined as "the right to control information about oneself;"[26] "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others;"[27] or simply, "the right to be let alone."[28] Although State statutes have recognized a panoply of privacy interests, the concept of privacy developed as common law is most often asserted against the press.[29]

Satellite and database technologies may change the very meaning of "public" and "private." As remote sensing satellites become more sophisticated, for example, it is possible that the average person's expectation of privacy could be eroded. Satellites are currently capable of spotting certain crimes, such as violations of environmental control laws. Eventually, satellites may be able to perform other functions, such as identifying and locating marijuana fields, or determining the inventories of manufacturers. In the far future, satellites may be able to monitor the activities of individuals.

Under current law, a person is protected against publicity given to facts about his or her private life. Although hard to define, the protections afforded by this right to privacy are clearly reduced when a person appears in public.[30] Mediasat could alter the current understanding of what the law regards as "appearing in public." Recently in *California v. Ciraolo*,[31] the Supreme Court decided that aerial reconnaissance was an acceptable law enforcement technique and that activities taking place in the defendant's backyard were in "plain view," even though they were surrounded by a 10-foot-high fence. Applying *Ciarolo*'s logic broadly, one could argue that citizen's have no right of privacy for any activity that might be seen from an airplane or satellite.

Computer databases may also change the meaning and expectations of privacy. The press may take advantage of the storage, re-

[25]The seminal article by Louis D. Brandeis and Samuel Warren, "The Right to Privacy," 4 *Harvard Law Review* 193 (1890), which structured subsequent debate, litigation, and legislation on privacy in the United States, was a reaction to the editorial practices of the Boston newspapers: "The press is overstepping in every direction the obvious bounds of propriety and decency . . . To occupy the indolent, column upon column is filled with idle gossip, which can only be procured by intrusion into the domestic circle. . . ." When the Warren/Brandeis theory of privacy was rejected in the first major case to consider it, *Roberson v. Rochester Folding Box Co.*, 171 N.Y. 538, 64 N.E. 442 (1902), the New York legislature reacted by creating a statutory right of privacy, New York Civil Rights Law, §§ 50 and 51.

[26]This definition forms the basis for the Privacy Act of 1974, Public Law 93-579, 5 U.S.C. §552(a).

[27]Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1967), p. 39.

[28]Brandeis and Warren, op. cit.

[29]Common law invasion of privacy is subdivided into four separately actionable torts: intrusion, disclosure, false light, and appropriation. William L. Prosser, "Privacy," 48 *California Law Review*, 383 (1960). Of particular concern for the present discussion is the tort of "public disclosure of private facts," which requires that the information made public by the press be in fact private, that the disclosure be highly offensive to a reasonable person, and that the subject matter of the disclosure not be of legitimate concern to the public.

[30]Hanson, *Libel and Related Torts*, §260 (1969).

[31]106 S.Ct. 1809 (1986). *Ciraolo* was a criminal case involving a warrantless search. As such, its reasoning may not be directly applicable to civil suits for invasion of privacy.

trieval, and processing capabilities of modern computer technology to construct comprehensive pictures of an individual from a myriad of transactional details—much as a mosaic painting is constructed from smaller pieces of no artistic significance in and of themselves. This capability was not practical in the world of print, where storing, retrieving and collating a mass of trivial detail was inefficient and wasteful, even when possible. Computer databases permit one person to fabricate whole new bodies of knowledge out of heretofore unconnected pieces of information. Much of the information about an individual's life is not, when taken in isolation, intimate or confidential. Purchasing merchandise at a department store, traveling on holiday, visiting the doctor, joining an association, reading a newspaper—these activities are often done in the open, and are available to anyone who cares to watch.

Although the press may, in certain instances, be liable for the collection or publication of personal information, this liability may conflict with the freedom of the press, especially when the information collected is available through public sources. In *Cox Broadcasting Corp. v. Cohn*,[32] the Supreme Court struck down a Georgia statute that barred publication of the names of rape victims. Although the Court recognized that "there *is* a zone of privacy surrounding every individual, a zone within which the State may protect him from intrusion by the press," it said that State may not censor "judicial records which are maintained in connection with a public prosecution and which themselves are open to public inspection."[33] The Court limited its ruling to court records,[34] but also said that:

> Public records by their very nature are of interest to those concerned with the administration of government, and a public benefit is performed by the reporting of the true contents of the records by the media. The freedom of the press to publish that information appears to us to be of critical importance to our type of government in which the citizenry is the final judge of the proper conduct of public business.[35]

Whether this First Amendment right of the press to publish court records also applies to other public records and publicly available information in general remains to be determined.[36] The problem has not been of widespread concern, in part because until recently one of the best barricades against breach of privacy was the difficulty and impracticability of integrating all of the public data about a person. Records such as arrest and prosecution data, credit status, purchases, mortgages and property records, hospital admissions, travel information, associational behavior, banking activity, and previous appearances in newspapers or on television were either uneconomical to keep for long periods of time, inaccessibly "buried" with thousands of other records, geographically dispersed, or not cross-referenced.[37]

The conflict between privacy and press freedoms may be most acute in cases where the government acts on behalf of the individual's privacy to foreclose the revelation of information that is normally public. In the case of sat-

[32]420 U.S. 469 (1975).

[33]Ibid.

[34]The Court declined to decide the more general question whether "the State may ever define and protect an area of privacy free from unwanted publicity in the press," and instead focused on the narrower question concerning publicly available judicial records.

[35]420 U.S. 469 (1975) at 32.

[36]In *Virgil v. Time, Inc.*, 527 F.2d 1122 (9th Cir. 1975), cert. denied 425 U.S. 998 (1976), the Ninth Circuit Court rejected the notion that the press has a First Amendment right to publish all private facts that are publicly available (in this case, facts drawn from an interview of the plaintiff). Only if the facts are newsworthy or of legitimate public concern would the press' First Amendment defense obtain.

[37]The new power to aggregate information was illustrated last year when two prominent businessmen were competing publicly to buy a major U.S. newspaper company. An enterprising journalist ran a check on both their names in Mead Data Central's NEXIS database, and learned that one of them, who lived in Indiana, was married to the sister of the investment banker representing the target newspaper's interests. He also learned that the Indiana man had just returned from a weekend with his wife in Mexico City, where the competitor lived. The two men announced a few days later that they were joining forces to buy the newspaper together, leading the journalist to report that the businessmen were colluding, rather than competing. Christopher Burns, "*Freedom of the Press in the Information Age*," OTA contract report, Apr. 21, 1987, p. 20.

State policy concerning the expungement of records on individuals may be ineffectual, because it must yield to freedom of the press.

ellite surveillance, for example, government might forbid press acquisition of private or proprietary pictures through remote sensing. This would undoubtedly be assailed as a "prior restraint" on press freedoms. The doctrine of prior restraint[38] holds that advance limitations on protected speech may not be "predicated on surmise or conjecture that untoward consequences may result."[39] Constitutional issues concerning prior restraint arise most often where the government acts to protect national security.

The State or Federal Government may act on behalf of individuals' privacy rights in ways that conflict with press access to information held in public or private databases. Many States, for example, have "expungement" statutes that apply to criminal or other records, which typically require that records be destroyed after a certain period of time, or when a defendant in a criminal case is acquitted. The theory behind the statutes is that an offender, once rehabilitated, deserves a chance to be free of his past and start anew.

If interactive electronic services are considered analogous to cable operators or newspapers, then they may, like cable and newspapers, claim First Amendment protection.

However, because more and more information is created or accessed in machine-readable form, and because the costs of storing it in that form are plummeting, newspaper morgues are growing in size and comprehensiveness. The question therefore arises whether the press will be required to expunge records that were once public and are now kept in its own files. Recent Supreme Court decisions suggest that no such requirement could be imposed on the press, especially if it carries a criminal penalty.[40] In some cases, State policy concerning the expungement of records on individuals may be ineffectual, because it must yield to freedom of the press.[41]

When information is not only *stored* and *accessed*, but also *provided* by the press electronically, further complications ensue. In interactive electronic services which provide information and services to the home, the use of the service by the consumer/reader also generates information for the provider about reading, viewing, and consumption patterns. This information can in turn be used to target and tailor information, such as advertising, that is fed back to the consumer. According to one author:

> Every transaction which is executed, and every page of information or service which is delivered, will generate its own electronic (machine-readable) record. The return channel in an interactive system will perform double labor for the interactive services industry; not only will it facilitate consumer requests for services, and thereby stimulate consumption, it will also transmit back to industry much relevant information concerning the modalities of consumer demand and consumption.[42]

Early concerns about privacy pertaining to the collection and sale of transactional information generated by the electronic press were ad-

[38]A prior restraint is government censorship. Other forms of liability or punishment for speech are imposed after the harm caused by the speech has occurred. Prior restraint, in contrast, is a prohibition of speech or publication before it occurs. "Any system of prior restraints of expression comes to this Court bearing a heavy presumption against its constitutional validity." *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 70 (1963); see also *New York Times Co. v. United States*, 403 U.S. 713 (1971), and *Near v. Minnesota*, 283 U.S. 697 (1931).

[39]*New York Times Co. v. United States*, 403 U.S. 713 (1971), Justice Brennan concurring at 724.

[40]See *Landmark Communications v. Virginia*, 435 U.S. 829 (1978); and *Smith v. Daily Mail Publishing Co.*, 443 U.S. 97 (1979).

[41]*Shifflet v. Thomson Newspapers, Inc.*, 431 N.E.2d 1014, 8 Med.L.Rptr. 1199 (1982).

[42]Kevin Wilson, "The Videotex Industry: Social Control and the Cybernetic Commodity of Home Networking," *Media, Culture, and Society*, vol. 8, 1986, pp. 7, 25. (Hereafter referred to as "Cybernetic Commodity.")

dressed in the Cable Communications Policy Act of 1984.[43] And, the Privacy Commission, whose recommendations were in large part adopted by Congress in the Privacy Act of 1974, suggested principles for the use of information gained through interactive electronic services. However, the Supreme Court has decided that individuals have no inherent legal interests in personal records owned by third parties.[44]

But privacy may only be part of the problem. The use of interactive information systems to provide the press with a precise consumer stimulus/response mechanism suggests to some that "improved techniques of social management are on the technological horizon . . . creating a truly cybernetic[45] cycle of production and consumption."[46] The difference between such cybernetic control and the familiar television or newspaper advertisement may be simply a matter of the degree of precision and power that electronic systems provide. Moreover, a greater sensitivity to consumer preferences may be generally desirable. Limiting the cybernetic control of consumer preference is more likely to be a political decision than a judicial issue. However, a question could also arise as to whether the collection and feedback of information through interactive services is protected speech, and thus whether this "cybernetic cycle" is an activity protected by the First Amendment. If interactive electronic services are considered analogous to cable operators or newspapers, then they may, like cable and newspapers, claim First Amendment protection. What information to provide to which consumers may be a matter of editorial discretion protected by the First Amendment.[47]

[43]47 U.S.C. §631.

[44]*U.S. v. Miller* 425 U.S. 435 (1976).

[45]The term, "cybernetic," comes from control theory and refers to systems that are highly adaptive, responding to their environment by sensing changes and responding by altering the environment or their response or both. In this case, a cybernetic cycle is one in which the electronic media, by virtue of its individualized and rapid interaction, not only adapts itself to individual consumers wants, but also acts to influence those wants.

[46]"Cybernetic Commodity" at page 35. See also Deanna Collingwood-Nash, and John Smith, *Interactive Home Media and Privacy*, report prepared for the Office of Planning, U.S. Federal Trade Commission, 1981.

[47]*Miami Herald v. Tornillo*, 418 U.S. 241 (1974).

IMPLICATIONS FOR NATIONAL SECURITY

Where the press seeks to gather information concerning national security, whether through satellite surveillance or computer databases, there is a potential for conflict between national security policies and the First Amendment. With satellite images, for example, the press could:

- disseminate information regarding U.S. military operations, thereby depriving U.S. troops of the critical element of surprise;
- reveal information considered sensitive by foreign governments, thereby prompting them to retaliate against U.S. Government activities, assets, or personnel;
- provide valuable intelligence to countries currently lacking their own reconnaissance satellites;

The Federal Government may attempt to limit access to or use of satellite imagery by the press.

- reveal facts about an unfolding crisis, making it more difficult for government leaders to act calmly and responsibly; and
- misinterpret satellite data in such a way as to precipitate a crisis.[48]

In response to these potentials, the Federal Government may attempt to limit access to or use of satellite imagery by the press. In the

[48]Taken from OTA, *Newsgathering From Space*, op. cit, p. 4.

case of a dedicated "Mediasat," it might do so permanently, through the licensing procedures established in the 1984 Landsat Act,[49] or temporarily, during a crisis, by limiting the resolution of the satellite's sensors, the images the satellite is allowed to collect, or the images the press is allowed to disseminate. Any of these options may run afoul of the doctrine of prior restraint. Prior restraints are allowed only if necessary to prevent "direct, immediate, and irreparable damage to our Nation or its people."[50] The outcome of such a challenge would turn on the exact nature of the Government limitations and the Supreme Court's ultimate determination of the status of newsgathering under the Constitution.

Similar First Amendment difficulties may be encountered with attempts to suppress or limit access to information in computerized databases. The ability of electronic information systems to construct revealing mosaic pictures from many smaller pieces of information has many parallels to the situation underlying the case of *United States v. The Progressive, Inc.*[51] In that case, *The Progressive* magazine proposed to publish an article on "The H-Bomb Secret: How We Got It, Why We're Telling It," which was derived entirely from public domain, unclassified sources. The Federal Government sought, and was granted, an injunction barring publication of the article under the Atomic Energy Act.[52] Notwithstanding the fact that the injunction constituted prior restraint—the most severe abrogation of First Amendment rights—and the fact that most of the research for the article was done in freely accessible government libraries,[53] the court held that the various sources of information, "*when drawn together, synthesized and collated*. . . . acquires the character of presenting immediate, direct, and irreparable harm to the interests of the United States"[54] (emphasis added).

Although the *Progressive* case did not involve computer databases, the enhanced ability of computer systems to achieve the same "aggregation and synthesis" of unclassified materials was at the heart of a recent public debate concerning *National Security Decision Directive 145* (NSDD-145).[55] The efficiency with which online databases can construct mosaic information was, in part, the rationale behind NSDD-145, which, among other things, established a "sensitive, but unclassified" category for information in government databases, and perhaps privately owned commercial databases as well.[56] NSDD-145's focus on electronic storage and retrieval systems recognized that databases store information that "even if unclassified in isolation, often can reveal highly classified and other sensitive information when taken in aggregate."[57]

The Federal Government proposed taking measures to protect sensitive information from hostile governments, including screening database entries, precluding the electronic publication of certain databases, providing database subscriber lists to the government, and/or limiting foreign subscriber access.[58] Some of these proposed measures may raise constitutional issues.[59]

[49]15 U.S.C. §§4201-4292.

[50]*New York Times Co. v. United States*, 403 U.S. 713 (1971), Justices Stewart and White, concurring.

[51]467 F.Supp. 990 (W.D. Wisc. 1979). The *Progressive* case is discussed in part I, ch. 2, of this report.

[52]68 Stat. 919, 42 U.S.C. 2011-2296.

[53]See: Rita Ann Reimer, *Legal and Constitutional Issues Involved in Mediasat Activities* (Washington, DC: Congressional Research Service, The Library of Congress, 1987), Report No. 86-823A, p. 12.

[54]467 F.Supp. 990, at 996.

[55]NSDD-145, Sept. 17, 1984.

[56]As of January 1987, the status of NSDD-145 with respect to commercial databases had not been clarified. For a more detailed discussion of NSDD-145, and related executive and legislative actions, see part II, ch. 4 of this report.

[57]National Policy on Protection of Sensitive but Unclassified Information in Federal Government Telecommunications and Automated Information Systems, NTISSP No. 2, Oct. 29, 1986 (hereafter cited as "National Policy"). This perception was echoed in a CIA Report, *Soviet Acquisition of Militarily Significant Western Technology: An Update* See part I, ch. 3 of this report.

[58]NASA has already implemented an access policy which restricts access with respect to foreigners, and members of the Air Force have visited several commercial database vendors asking for subscriber lists. See *Scientific Information*.

[59]For example, the Federal Government has a right to create conditions on access to, or publication of, governmentally funded information, so long as they do not conflict with the Freedom of Information Act, 5 U.S.C. §552(a). Moreover, as we have seen, the Supreme Court has not recognized a constitutional right of the press to *gather* information, so it is unlikely

continued on next page

The Federal Government proposed taking measures to protect sensitive information from hostile governments, including screening database entries.

Prior restraint on commercial database publishers raises peculiar problems for the traditional theories under which prior restraint is permissible. Individual database entries do not necessarily pose a threat to national security that would justify restraining them. It is ostensibly the concatenation of individual database entries that raises national security concerns, but this concatenation may not be specifiable before a given database search. Yet judicial precedent with prior restraint has, without exception, concerned a single publication, the contents of which could be known ahead of time.

Prior restraint issues normally arise when the government seeks an injunction prohibiting publication. But, even alternative approaches to national security problems of database mosaics may pose constitutional issues. In the case of NSDD-145, for example, sensitive but unclassified information is defined as "information the disclosure, loss, misuse, alteration, or destruction of which could adversely affect national security or other Federal Government interests."[60] But database vendors may have little clue as to whether the data that they sell could "adversely affect national security" until it is conjoined with other data; the "sensitivity" of information in a database will depend on its combination with other information. Attempts to control disaggregated data may therefore run afoul of the "vagueness" doctrine, which is based on the due process clause of the 14th Amendment, and which requires that a statute "neither forbid nor require the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application."[61] Vague laws may also infringe upon the First Amendment rights of the press by "chilling" protected expression.

continued from previous page
that the press, as database *users*, would be able to assert a constitutional interest in access to sensitive information.

[60]From "National Policy," Section II—Definition.
[61]*Zweiker v. Koota*, 389 U.S. 241 (1967).

Chapter 2

New Technologies for Editing and Selecting News and Information

Far more information is produced than consumed. Measuring information in words, one census found that, on average, over 11 million words are made available to Americans over print and electronic media each day, and this figure has been growing at roughly 8 percent each year since 1980. Of these words supplied, only about 48,000 were actually read or heard by any one individual (on average).[1] Editors, whose task it is to gather, select, and organize this welter of information for particular purposes or consumers, are more crucial to the information consumer than ever. As one commentator has observed, "in the Age of Information, editors assume an even greater importance; people will pay *not* to be deluged with unedited data."[2]

For the electronic publisher, exercising responsibility for identifying, verifying, and policing sources of information may become difficult or impossible, raising questions about standards of liability.

[1]Ithiel de Sola Pool, et al., *Communications Flows: A Census in the United States and Japan* (New York, NY: Elsevier Science Publishing Co., 1984), p. 16. Survey years 1960-1980.

[2]Bruce Owen, "The Role of Print in an Electronic Society," *Communications for Tomorrow: Policy Perspectives for the 1980's*, G. Robinson (ed.) (New York, NY: Praeger Publishers, 1978); as quoted in Mark Nadel, "Editorial Freedom: Editors, Retailers, and Access to the Mass Media," 9 *Comment: Hastings Journal of Communications and Entertainment Law* 213 (winter 1987), which provides a useful discussion of the role and functions of editors.

It does not follow from this, however, that editing will continue to be a centralized activity, nor one conducted solely by people. Quite the contrary: the deluge of information made possible by electronic publishing technology may require technological methods of sorting information for relevance and importance. Technologies such as expert systems are emerging, which when used in conjunction with electronic publishing, can disperse editorial control to the recipients, rather than the originators, of news stories and information. Citizens may come to see "news stories" not as a standardized, authoritative, and "balanced' text, but as a largely self-selected collection of sources to be assayed in context.

The emerging electronic publishing industry will pose unique questions concerning editorial control and responsibility under the First Amendment. Traditional assumptions about the press' editorial responsibility for the information it publishes may be drawn into question. The First Amendment serves to insulate responsible press conduct from liability in the interest of robust debate on matters of public importance. But for the electronic publisher, exercising responsibility for identifying, verifying, and policing sources of information may become difficult or impossible, raising questions about standards of liability for what is carried over phone and coaxial cable lines. Electronic publishing also challenges traditional distinctions between publishers and common carriers, further complicating questions of liability and First Amendment protections.

ELECTRONIC PUBLISHING

Electronic publishing combines information access and retrieval capabilities with messaging and transaction services. It is a point-to-point communication system in which text, audio, or video information may be carried by telephone network, microwave transmission,

satellite relays, or even coaxial cable television lines. It is roughly equivalent to what the Justice Department calls "information services" and the Federal Communications Commission calls "enhanced services."[3] Within the ambit of electronic publishing are teletext,[4] videotex,[5] electronic mail,[6] electronic bulletin boards,[7] and electronic transactional services, such as home shopping and home banking.[8] Although there are substantial differences between the types of electronic publishing (teletext, for example, is broadcast, while videotex is telephonic), they will be referred to collectively as electronic publishing.[9]

Excluded from present consideration is broadcast radio or television, cable television, unenhanced voice telephony (i.e., exclusive of voice-mail storage and forwarding systems), and conventional print publishing. The distinction between electronic publishing and conventional communications, such as TV or radio, is somewhat artificial, but suited to present analyses. In the long run, the convergence of modes of communication will destroy distinctions between electronic publishing and other forms of publishing; "the one-to-one relationship that used to exist between a medium and its use is eroding. This is what is meant by the convergence of modes."[10]

Electronic publishing may look like a different kind of service at different times, depending on the use the subscriber makes of it. It may function like conventional mail at one time; book or newspaper publishing at another; a bulletin board with messages pinned to it at another; a conference room at another; or even a bank or retail store at another.

In the long run, the convergence of modes of communication will destroy distinctions between electronic publishing and other forms of publishing.

Moreover, electronic publishing networks can be "nested" within other networks; a serv-

[3]In *United States v. AT&T Co.*, 552 F.Supp. 131, 181 (D.C. Cir. 1982), *affirmed* 103 S.Ct. 1240 (1983) (Modified Final Judgment), Para IV J, "information services" were defined as "the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information which may be conveyed via telecommunications." In *Computer II*, 77 F.C.C. 2d 384, at 498, "enhanced services" are "services, offered over common carrier transmission facilities used in interstate communication, which (1) employ computer processing applications that act on the format, content, code, protocol or similar aspects of the subscriber's transmitted information; (2) provide the subscriber additional, different or restructed information; or (3) involve subscriber interaction with stored information."

[4]Teletext is a one-way broadcast transmission of textual information, using the Vertical Blanking Interval (VBI) of a conventional television signal. Data is transmitted to a subscriber's television from a central computer, and the viewer selects from "pages" of information. Teletext requires a decoder, attached to a television set, to be received. The most common form of teletext transmission in the United States is closed-captioning for the hearing impaired. See: Efrem Sigel, *The Future of Videotext* (White Plains, NY: Knowledge Industry Publications, 1983); Richard Neustadt, *The Birth of Electronic Publishing* (White Plains, NY: Knowledge Industry Publications, 1982); Neustadt, Skall & Hammer, "The Regulation of Electronic Publishing," 33 *Federal Communications Law Journal* 331 (1981); and Anne Branscomb, "Electronic Publishing: A Global view of Videotex," 36 *Federal Communications Law Journal* 119 (1984).

[5]Videotex differs from teletext in several ways: it is "interactive," in that information flows in two directions, from the user to the host computer and back again; information is typically organized by search, rather than by preset pages; there is no theoretical limit on the amount of information that can be transmitted and stored; and videotex is normally transmitted via contained media (i.e., telephone or cable lines) in digital, computer-processable form. For present purposes, videotex includes networks accessed by personal computer, such as The SOURCE, CompuServe, LEXIS, NEXIS, WESTLAW, and ARPANET, as well as television-adapted networks, such as the experimental Viewtron, Keyfax, Trintex, and "dedicated" network systems such as the Telidon (Canada), Minitel (France), and Prestel (England) systems.

[6]Electronic mail is an electronically transmitted message from one computer terminal to another, usually via a host computer, which stores and routes the message. Electronic mail is commonly available in most videotex services. Current electronic mail services include MCImail, CompuServe, the SOURCE, GTE Telemail, and Western Union EasyLink.

[7]An electronic bulletin board is a publicly accessible videotex computer file, which is typically organized into "conferences" or "topics" that users may create and join, or limit membership to. See note 5 above.

[8]Home banking, for example, allows a customer to handle electronic funds transfers from his or her own computer. The first system in the United States was Chemical Bank's "Pronto" system, which began in September 1983. See: U.S. Congress, Office of Technology Assessment, *Effects of Information Technology on Financial Service Systems* (Springfield, VA: National Technical Information Service, September 1984).

[9]See p. 15 of this report for a discussion of the distinction between electronic publishing and database services.

[10]Ithiel de Sola Pool, *Technologies of Freedom* (Cambridge, MA: Belknap Press, 1983), p. 280.

ice for routing messages from one location to another may be added on top of a network providing for their storage, which may itself lease lines and switching service from one or more networks. Members of these various networks can also "talk" to each other between otherwise self-contained networks.[11]

Electronic publishing is also interactive; unlike all previous media used by the press, where the journalistic product was a single package whose contents and priorities were controlled by editors, many electronic publishing systems permit the style, organization, order, and content of the items to be selected by the user, rather than the publisher. The converse is also true: writers and publishers may choose their readers, and differentiate their products across classes of readers.[12]

Interactivity means, moreover, that users can themselves become reporters or publishers. This feature is of great significance for the question of "who is press," and it also suggests that the *sources* for news and information may in the future become dispersed, and less subject to centralized control by the electronic publisher. A paper publishing system which today looks something like this:[13]

Source(s) • Reporter • Publication • Distribution • Point of Sale • User

may one day be joined by an electronic publishing system that looks more like this:

Source(s) • Interconnection • User

These features of electronic publishing—the decentralization of editorial control, the multiplicity of versions of news and information products, the loss of an authoritative text, the many roles of electronic publishers, the dispersion of news and information sources—raise significant questions about liability for false, inaccurate, defamatory, indecent, obscene, and infringing information. Holding the electronic publisher liable for injurious information[14] entails conflicts with the "profound national commitment" made in the First Amendment "to the principle that debate on public issues should be uninhibited, robust, and wide open . . ."[15]

[11]These internetwork links are known as "gateways." See J. Quarterman and J. Hoskins, "Notable Computer Networks," *Communications of the ACM*, vol. 29, October 1986, pp. 932-971, for a good summary of computer networks and related concepts.

[12]The press has already begun this differentiation process with, for example, the publication of domestic and international versions of *Time* and *Newsweek*, inclusion in newspapers of supplements aimed at suburban readers, and the circulation of *TV Guide* to different viewing audiences. Electronic publishing will enable finer distinctions along different classificatory lines.

[13]From an OTA staff conversation with Mr. R. Taylor Walsh, Electronic Information Services Development, Silver Spring, MD.

[14]The term "injurious information" will be used to refer to defamation, negligence, copyright infringement, fraud, invasion of privacy, intentional infliction of emotional distress, and other uses of information that cause pecuniary, emotional, reputational, or bodily harm. This is in accordance with a recent appeals court decision that held that "First Amendment protections apply to all actions whose gravamen is injurious falsehood." *Blatty v. New York Times, Inc.*, 12 Med.L. Rptr. 1928 (2nd Cir. 1986), cert. denied, No. 86-1803) (1987).

[15]*New York Times v. Sullivan*, 376 U.S. 254 (1964).

EDITORIAL CONTROL AND LIABILITY

The editorial decisions of the press go to the heart of the First Amendment protection of its freedom. As the Supreme Court said in *Miami Herald Publishing Co. v. Tornillo*,[16]

> The choice of material to go into a newspaper, and the decisions made as to the limitations on the size and content of the paper, and treatment of public issues and public officials—whether fair or unfair—constitute the exercise of editorial control and judgment. It has yet to be demonstrated how governmental regulation of this crucial process can be exercised consistent with the First Amendment guarantees of a free press as they have evolved to this time.

A corollary to editorial *freedom* is editorial *responsibility*; under common law, the exercise of editorial discretion over whether and what to publish is the basis for liability for defa-

[16]418 U.S. 241 (1974).

mation and other forms of injurious information.[17] An assumption underlying conventional theories of press liability is that the press—be it newspaper, journal, magazine, radio, or television—is capable of exercising editorial discretion over the content of its publications. Where the press is required by law to accept content "as is," it is generally absolved from responsibility for damages caused by false or inaccurate publication.[18] Where a medium is treated by law as a common carrier, and is therefore forbidden from discriminating against any speaker or otherwise exercising editorial control, it is absolved of any legal responsibility for statements made over the medium.[19]

This simple symmetry between control and liability may become hard to apply to electronic publishers. On a network, electronic publishers may resemble conventional print publishers insofar as they can or do choose which speakers may use their services.[20] They may in fact choose *who* shall "speak," but they are less often in control over *what* is said over the network. The choice of who speaks may be made explicitly—as where a computer network contracts with news or database services for the provision of information to subscribers.[21] Or, it may be made tacitly, and involve nothing more than permitting subscribers to speak, or allowing the creation of bulletin board conferences.

An assumption underlying conventional theories of press liability is that the press is capable of exercising editorial discretion over the content of its publications.

Whether an electronic publishing service should or can bear liability for information distributed on its service is a matter of some constitutional consequence. If, in lieu of action by Congress or the Supreme Court, the Federal Communications Commission (FCC) were to decide that electronic publishing is beyond its jurisdiction as being neither "ancillary" to broadcasting, nor common carriers (and thus not relieved from publisher liability),[22] an argument can be made that it should be treated in the same way as print publishers. The question then is whether the electronic publisher *can*, as a practical matter, exercise the same control as these other types of publishers,[23] and if requiring it to do so will inhibit the content of or access to the system. In order to

[17]As with torts generally, the basis for liability for "informational torts," such as defamation, negligent misrepresentation, fraud, and even product liability, is that of misfeasance; that is, once one undertakes a discretionary action, such as publication, one is bound to exercise reasonable care in carrying it out. Although the press is, in certain instances, no longer strictly liable for what it publishes, *New York Times v. Sullivan*, 376 U.S. 254 (1964) and *Gertz v. Robert Welch, Inc.*, 418 U.S. 323 (1974), the basis for liability for defamation, invasion of privacy, and negligent misrepresentation remains an intent to publish. Where the exercise of editorial judgment and control in conveying or publishing information is prohibited by law—as is the case with common carriers such as telephone and postal services—there is no liability for the information.

[18]For example, where a broadcaster is required by law to provide "equal time" for the responses of political candidates, it will not be held liable for defamatory statements made in the response. *Farmers Educational Cooperative Union of America v. WDAY*, 360 U.S. 525 (1959).

[19]*National Association of Broadcasters v. FCC*, 740 F.2d 1190 (D.C. Cir. 1984).

[20]For example, services such as THE SOURCE, LEXIS, NWI, and CompuServe contract with selected newswire services to provide information to their subscribers. Some electronic publishers, while they do not themselves provide particular news services, may allow such services to be "ported" from another online source to their own. National security directives may eventually force videotex providers to exclude some potential users.

[21]For example, West Publishing contracts with Dow Jones News Retrieval Service to enable WESTLAW subscribers access to Dow Jones' financial analyses and news services.—

[22]*Telecommunications Research and Action Center v. FCC*, 13 Med. L. Rept. 1881 (D.C. Cir. 1986)

[23]On networks that provide bulletin board and news and information services, there may be literally hundreds and thousands of new messages each day. They may come in faster than any publisher could scan them. Even if such scanning were possible, controlling what is posted may be impossible. "To control what is posted on a network, it is necessary to control access to that network. Most existing networks are not strong on security. The safest policy in using networks is to assume that any network can be broken, that any transmission can be recorded, and that most can be forged." J. Quarterman and J. Hoskins, "Notable Computer Networks," *Communications of the ACM*, vol. 29, October 1986, p. 967.

avoid civil liability for defamation, negligence, or infringement of copyright, or criminal liability for fraud or theft, the electronic publisher may be forced to censor what is written to its host computer.

The spectre of "self-censorship" has caused the Supreme Court, on several occasions, to recognize First Amendment privileges that effectively limit the circumstances under which newspapers and broadcasters will be held liable.[24] Electronic publishing raises the question whether the limited types of privileges now granted the press will be adequate to avoid self-censorship. Monitoring the accuracy and truthfulness of all of the information posted to a computer conference, for example, may well be beyond the system operator's abilities. The press, in becoming electronic, may require more latitude for error than conventional print publishers.[25]

[24]Beginning with *New York Times, Inc. v. Sullivan*, 376 U.S. 254 (1964) and culminating in *Gertz v. Welch*, 418 U.S. 323 (1974), the Supreme Court fashioned First Amendment-based press privileges with respect to defamatory speech concerning public officials and public figures. In *Rosenblatt v. Baer*, 383 U.S. 75 (1966), the Court recognized a similar privilege with respect to speech that is invasive of individuals' privacy.

[25]Of course, the sources of information posted on a computer network may also be held liable for injurious information. While straightforward in theory, this may be difficult to implement in practice. Database providers to the network offer thousands of "pieces" of information, most of which they have no involvement in creating; mediated by artificially intelligent "front ends," information may come to consumers that is a machine-compiled synthesis of many sources, which may themselves not be cited in the allegedly defamatory or negligent report; and the long and complex chains of distribution that are possible in value-added networks may give a totally different and often circuitous meaning to the nature of what counts as a "fact" or the "truth" for purposes of verification of information. See generally, Ithiel de Sola Pool, *Technologies of Freedom*, ch. 7 (Electronic Publishing) and Anthony Smith, "Information Technology and the Myth of Abundance," *Daedelus*, vol. 111, fall 1982, pp. 1-16.

The question whether the privileges extended the press also apply to "nonmedia" defendants, i.e., to individual citizens, and whether a distinction between media and nonmedia defendants can be made at all, is crucial to the extent of First Amendment protections afforded electronic publishers. The Supreme Court was recently urged to hold nonmedia defendants to a higher standard of conduct than the media, but it avoided the issue entirely, holding instead that press privilege against defamation extended only to "matters of public concern" (an incorrect credit report was held not to be a matter of public concern).[26] However, because conventional print and broadcast media are in great part responsible for defining what constitutes a protected "matter of public concern," that question may hinge on the medium of communication, after all. The role of technology in expanding who constitutes "the press" was recognized by Justice Brennan who wrote in his dissent that:

> "[f]irst amendment difficulties lurk in the definitional question such an approach would generate. And the distinction would likely be born an anachronism. (Brennan's footnote): Owing to transformations in the technological and economic structure of the communications industry, there has been an increasing convergence of what might be labeled "media" and "nonmedia."[27]

[26]*Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749 (1985). In a recent State court decision, *Culliton v. Mize*, 403 N.W.2d 853 (1987), the court held that the First Amendment privileges recognized in *New York Times v. Sullivan* apply to nonmedia defendants.

[27]472 U.S. 749 (1985) at 34.

GLOBAL NETWORKS AND THE INTERNATIONAL PRESS

Electronic publishing may blur distinctions between "domestic" and "foreign" press. Internetworking (communicating between two or more networks), in combination with global communications satellites, the emergence of "metanetworks," and the eventual conformance of worldwide communications protocols, makes the concept of a "purely domestic" electronic publisher an anachronistic term. Except with respect to cost, geography is largely irrelevant to modern telecommunications systems.

Congress and the courts may eventually have to confront the question of whether First Amendment rights extend to the foreign press publishing in the United States. The question may take many forms—whether standards of liability will apply to foreign-originated transmissions, whether domestic regulations apply, whether import/export laws conflict with First Amendment rights, or whether control, even if permitted under the First Amendment, is possible.[28]

The First Amendment status of the foreign press, and foreign speakers in general, is one of the least understood areas of First Amendment jurisprudence. A case involving deportation of aliens for allegedly subversive speech under the McCarran-Walter Immigration Act of 1952 is currently pending before a Federal court.[29] In the only case on point, *Times Newspapers Ltd. (Of Great Britain) v. McDonnell Douglas Corp.*,[30] the court held that *The Sunday Times of London*, an English newspaper with offices and a small circulation in the United States, was protected from having its publication suppressed. The court said that freedom of the press is not limited to what is published in America for American readers, but was also "designed to protect the rights of readers and distributors of publications no less than those of writers or printers."[31]

Congress and the courts may eventually have to confront the question of whether First Amendment rights extend to the foreign press publishing in the United States.

Though the right of foreign journalists to publish in the United States is not yet firmly established in constitutional law, the right of readers, viewers, and listeners to receive news and information has been established in other contexts, and may be indirectly available to nonresident electronic publishers. Even this rationale, however, is tenuous; relying as it does on cases involving very specific circumstances and court dicta.[32] The fact that section 310 of the Communications Act requires that broadcast licenses be held only by citizens of the United States, and that a recent Supreme Court decision upholding registration and labeling requirements for Canadian made films,[33] suggests that the foreign press may have lesser First Amendment rights, if they have any.

Short of monitoring all international data traffic, there may be no way to stem news and information from foreign sources, even if it were desirable.

The political and legal impetus for recognizing First Amendment rights for the international press may not necessarily come from judicial interpretations of the Constitution; it may come from international authority, and from the interconnectedness of nations that has accompanied technological change.[34] For

[28]These issues belong to a class of emerging issues concerning "transborder data flows"; the movement of data between countries. For an overview of the legal and policy issues surrounding transborder data flows, see: A. Branscomb, "Global Governance of Global Networks: A Survey of Transborder Data Flow in Transition," 36 *Vanderbilt Law Review* 985 (1983).

[29]"Federal Judge Declines To Rule on Free Speech Rights of Foreigners," *New York Times*, May 21, 1987. The case of Margaret Randal is still pending as of December 1987.

[30]387 F.Supp. 189 (C.D. Cal. 1974).

[31]Id. Quoting *Quantity of Copies of Books v. State of Kansas*, 378 U.S. 205 (1964).

[32]In *Red Lion Broadcasting Co. v. FCC*, 395 U.S. 367 (1969), in the context of the constitutionality of the fairness doctrine, the Court said that "the people as a whole retain their interest in free speech . . . [it] is the right of viewers or listeners, not the right of the broadcasters, which is paramount." See also *Virginia State Board of Pharmacy v. Virginia Citizens Consumers Council*, 425 U.S. 748 (1976), *Board of Educ. v. Pico*, 457 U.S. 853 (1982); which are commonly cited as constitutional foundations for a right of the public to receive information under the First Amendment. See, e.g., Mark Nadel, "A Unified Theory of the First Amendment: Divorcing the Medium From the Message," 11 *Fordham Urban law Journal* 163, 187 (1982), and Emerson, "Legal Foundations of the Right to Know," 1976 *Washington University Law Quarterly* 1.

[33]*Meese v. Clarkson*, 55 U.S.L.W. 4586 (Apr. 28, 1987).

[34]This topic will be developed in a forthcoming OTA special bicentennial report on *Science, Technology, and Constitutional Governance*.

example, Article 19 of the Universal Declaration of Human Rights proclaims that:

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information *through any medium regardless of frontiers.*[35]

This does not have legal effect, but it is widely recognized as the basis for international law. Whether the foreign press may avail itself of First Amendment rights or not may become an academic exercise. Short of monitoring all international data traffic, there may be no way to stem news and information from foreign sources, even if it were desirable. A hoax on April Fools Day in 1984 on a computer network named USENET may be a harbinger of things to come—"kremvax!kgbvax!chernenko" joined the network.[36] (The notation is the name, address, and routing message used on the network.) As Leonard Marks, a former director of the U.S. Information Agency, couched the issue,

> Global electronic networks . . . will be effectively beyond the reach of the traditional forms of censorship and control. The only way to "censor" an electronic network moving . . . [at] 648 million bits per second is literally to pull the plug.[37]

In other words, the only effective means of controlling foreign speakers speaking in the United States may be to disable the communications abilities of American citizens,[38] an action that would directly raise First Amendment rights.

[35]Universal Declaration of Human Rights, G.A. Res. 217 (III) U.N. Doc. A/810, at 71, art. 19 (1948) (emphasis added); as quoted in John Eger, "The Global Phenomenon of Teleinformatics: An Introduction," 14 *Cornell International Law Journal* 203, 207 (1981).

[36]"Notable Computer Networks," *Communications of the ACM*, vol. 29, October 1986, p. 967.

[37]L. Marks, *International Conflict and the Free Flow of Information in Control of the Direct Broadcast Satellite, Values in Conflict* (Palo Alto, CA: Aspen Institute Program on Communications and Society, 1974); as quoted in J. Pelton, "The Technological Environment," *Toward a Law of Global Communications Networks*, Science and Technology Section of the American Bar Association, A. Branscomb (ed.) (New York, NY: Longman, 1986), pp. 37, 44-45.

[38]Though not in the context of foreign speech, this step is not unprecedented; computers and communications were confiscated from a system operator in 1984 whose communications facilities were used for telephone credit card fraud. "Free Speech Issues Surround Computer Bulletin Board Use," *New York Times*, Nov. 12, 1984, p. A1, col. 1.

Chapter 3

New Technologies for Publishing and Disseminating News and Information

THE CONVERGENCE OF THE MEDIA

Of all the First Amendment issues concerning the press and new technology, none is more contentious than Federal regulation of the means of publishing and disseminating news through electronic media. The seemingly absolute prohibition on abridgments of press freedom enunciated in the First Amendment ("Congress shall make no law . . .") has nevertheless been found compatible with a three-tiered system of communications freedom: print media, broadcast media, and common carrier. This separation was at first a product of market economics and agreements between key players in the communications industry,[1] rather than being mandated by technology.[2] It was nevertheless embodied in the regulations of the Federal Communications Commission (FCC).[3] Today, technology is ushering in a convergence of forms of press publishing that were once partitioned by technology: print publishing, mail, broadcasting, and telephone.

The seemingly absolute prohibition on abridgments of press freedom enunciated in the First Amendment has nevertheless been found compatible with a three-tiered system of communications freedom: print media, broadcast media, and common carrier.

Print media[4] occupy the first tier of constitutionally protected communication, and are subject only to laws concerning injurious speech (like defamation and negligence), constitutionally unprotected speech (obscenity and "fighting words"), and those laws regulating the press as a business, without regard to the press' communicative functions (e.g., corporate, labor, and antitrust laws).[5]

The broadcasting media occupy the second tier. Under the Communications Act of 1934, the FCC has the task of:

> . . . regulating interstate and foreign commerce in communication by wire and radio so as to make available, so far as possible, to all the people of the United States a rapid, efficient, nationwide and worldwide wire and radio communication service with adequate facilities at reasonable charges for the purpose of the national defense, for the purpose of promoting safety of life and property through the use of wire and radio communication.[6]

[1] "In 1926 AT&T abandoned broadcasting in return for RCA's commitment to use AT&T's lines rather than Western Union's for networking. The agreement provided for exchange of patent licenses, and WEAF was sold to RCA, where it became WNBC, the flagship station for the National Broadcasting Co." Ithiel de Sola Pool, *Technologies of Freedom* (Cambridge, MA: Belknap Press, 1983), p. 35. See also Lynn Becker, "Electronic Publishing: First Amendment Issues in the Twenty-First Century," 13 *Fordham Urban Law Journal* 801, 818-820 (1984).

[2] "Other approaches were proposed and tried. For a quarter of a century from 1893 phones carried music and news bulletins to homes in Budapest, Hungary. Thomas Edison thought that the main use for the phonograph he had invented would be for mailing records as letters. ". . . The fact that different technologies were consecrated to different uses protected media enterprises from competition from firms using other technologies." Pool, *Technologies of Freedom*, op. cit., p. 27.

[3] Congress provided for three distinct regulatory schemes: for *broadcasters* (47 U.S.C. §§ 301-332), *common carriers* (47 U.S.C. §§201-224), and for *non-broadcast users* (47 U.S.C. §§ 351-362). *Print media*, which do not travel by "wire or radio," are beyond the jurisdiction of the FCC to regulate. 47 U.S.C. §151.

[4] "Print media" refers not only to all paper and ink publications; it is coextensive with any "work fixed in a tangible medium of expression," as defined under the Copyright Act, 17 U.S.C. §102(a), and thus includes motion pictures, paintings, sculpture, photographs, computer-processible information (including programs and databases), and sound recordings.

[5] *Miami Herald Co. v. Tornillo*, 418 U.S. 241 (1974), has reaffirmed the premier position occupied by the print media, so far as freedom from government interference in editorial control is concerned.

[6] 47 U.S.C. §151.

80-645 - 87 - 3

In carrying out this responsibility, the FCC must conform its actions to those "consistent with the public interest, convenience [and] necessity."[7] Under this authority, and based on a rationale that "the electromagnetic spectrum is simply not large enough to accommodate everybody,"[8] the FCC licenses broadcasters and conditions the grant and renewal of licenses on compliance with a variety of content and structural regulations. These regulations include:

- *Cross-Ownership Restrictions*: In the interest of promoting diversity, the FCC imposes three general types of restrictions on multiple ownership of broadcasting facilities: those limiting ownership in a single community,[9] those limiting ownership of broadcast facilities by single entities nationwide,[10] and those forbidding newspapers from owning television stations in the same community in which they publish.[11]
- *The Fairness Doctrine*: Under FCC decisions construing a 1959 amendment to the Communications Act of 1934, broadcasters were obligated to "operate in the public interest and to afford reasonable opportunity for the discussion of conflicting views on issues of public importance."[12] The FCC added a further gloss to this statutory language in the Report Concerning General Fairness Doctrine Obligations of Broadcast Licencees, 102 F.C.C. 2d 143, 146 (1985): licensees must "provide coverage of vitally important controversial issues of interest in the community served by licensees . . . [and] provide a reasonable opportunity for the presentation of contrasting viewpoints on such issues." The codification of the Fairness Doctrine in the Communications Act (H.R. 1934) was recently vetoed by the President, and the FCC voted to repeal its fairness regulations on the ground that they offended the First Amendment.*
- *The Equal Time Doctrine*: "If any licensee shall permit any person who is a legally qualified candidate for any public office to use a broadcasting station, he shall afford equal opportunities to all other such candidates for that office in the use of such broadcasting station."[13]
- *Reasonable Access*: Broadcasters must allow "reasonable access . . . for the use of a broadcasting station by a legally qualified candidate for Federal elective office on behalf of his candidacy."[14]
- *Indecency*: Under criminal law and FCC regulations, broadcasters are held to a higher standard than other publishers, insofar as they are prohibited from broadcasting not only "obscene," but also "indecent" programming.[15] The rationale for this higher standard is that the broadcast audience, and particularly children, are "captive."[16]

FCC regulations, and indeed, much of the rationale under which the FCC regulates, have come under attack in recent years, largely as a result of technological challenges to the notion of scarcity.[17]

[7]47 U.S.C. §307.

[8]*National Broadcasting Co. v. United States*, 319 U.S. 190, 213 (1943). The scarcity rationale was reaffirmed as the basis for broad FCC authority to regulate in *Red Lion Broadcasting v. FCC*, 395 U.S. 367 (1969).

[9]47 CFR §§ 73.35 (AM), 73.240 (FM), and 73.636 (TV).

[10]Ibid.

[11]See Second Report and Order, Docket No. 18110, 50 F.C.C. 2d 1046 (1975).

[12]47 U.S.C. §315(a).

*56 U.S.L.W. 2112 (Aug. 25, 1987).

[13]47 U.S.C. §315.

[14]47 U.S.C. §312(a)(7).

[15]Broadcast of "obscene, indecent, or profane" language or images is a criminal violation, 18 U.S.C. §1464, for which the FCC may revoke a license, 47 U.S.C. 312(a)(6). This power was upheld in *FCC v. Pacifica Foundation*, 438 U.S. 726 (1978). The FCC recently recommended expanding the operative definition of "indecency" beyond seven particular words to include the generic definition of broadcast indecency advanced in *Pacifica*, which is: "language or material that depicts or describes, in terms patently offensive as measured by contemporary community standards for the broadcast medium, sexual or excretory activities or organs." The Commission added that "in certain circumstances, innuendo or double entendre may give rise to actionable indecency." 52 *Federal Register* 16386-01 (Tuesday, May 5, 1987).

[16]See, e.g., *Cohen v. California*, 403 U.S. 15 (1971)

[17]For example, see U.S. Congress, 98th Cong., 1st sess., Senate Committee on Commerce, Science, and Transportation, *Print and Electronic Media: The Case for First Amendment Parity*, printed at the direction of Hon. Bob Packwood, Chairman, for the use of the Committee on Commerce, Science, and Transportation, Senate (Washington, DC: U.S. Government Printing Office, 1983).

Whether broadcasting is a scarce resource depends to a great degree on how "scarcity" is defined. Absolute numerical comparisons of the number of media outlets may be misleading measures of scarcity. If scarcity is measured by the number of organizations or individuals wishing to broadcast as compared with the number of available frequencies, then scarcity is still the rule for broadcasting. There are, for example, no open broadcast television channels in the top 50 markets in the United States. If, as one First Amendment scholar suggests, scarcity occurs in situations where "one utterance will necessarily displace another," then scarcity takes on yet another meaning:

> . . . [the] opportunities for speech tend to be limited, either by the time or space available for communicating or by our capacity to digest or process information. . . . The decision to fill a prime hour of television with *Love Boat* necessarily entails a decision not to broadcast a critique of Reagan's foreign policy . . . during the same hour.[18]

The development of cable television (which typically carries anywhere from 34 to 120 stations), the direct broadcast satellite, other microwave communications systems, low power television, and other new technologies cast doubt on scarcity as the premise for government regulation. The broadcast medium far exceeds the print medium in sheer number of outlets.[19] Broadcasting has become more ubiquitous and far more diverse than newspapers in many metropolitan areas. Multiplexing and compression techniques may further overcome physical limitations of the electromagnetic spectrum, the limitations on time and space inherent to the broadcasting medium.

Whether broadcasting is a scarce resource depends to a great degree on how "scarcity" is defined.

In this context, the FCC has now rejected the scarcity rationale—at least as the basis for the fairness doctrine.[20] Many in Congress are seeking to legislate the fairness doctrine out of concern over the scarcity and high cost of broadcast outlets. The FCC has in other instances suggested an alternative rationale having to do with the broadcasting industry's "power to communicate ideas through sound and visual images in a manner that is significantly different from traditional avenues of communication because of the immediacy of the medium."[21]

Yet even these constraints on the broadcasting media are being overcome by technologies, the videocassette recorder, for instance, that permit an audience to select among and store programs of its choosing. The element of viewer selection and timing was a principal reason for the Supreme Court's finding that "time-shifting" television programs constituted "fair use" and is not a violation of copyright law.[22]

Common carriers, finally, are subject to yet different treatment under Federal law and the First Amendment. Under Title II of the Communications Act, communications common carriers are subject to franchise, rate, service, and reporting requirements, and "must hold themselves out to all comers" on a nondiscriminatory basis.[23] Thus common carriers are not

[18]Owen Fiss, "Free Speech and Social Structure," 71 *Iowa Law Review* 1405, 1412 (July 1986).

[19]At the end of 1985, there were 9,871 radio and 1,220 television stations operating in the United States, compared to 1,676 daily and 6,600 weekly newspapers, and more than 10,000 magazines. *Broadcasting Yearbook 1986*, and *Editor and Publisher Yearbook 1986*, as cited in Christopher Burns, *Freedom of the Press in the Information Age*, OTA contract report, Apr. 21, 1987, p. 20. In 1986, A.C. Nielsen counted 86 million television homes and a total of 157 million television sets in use, compated to 63 million daily newspaper subscribers. Television Bureau of Advertising, "Trends in Television, 1986," as cited in Burns, op. cit. In 1985, the average home had the television on 7 hours and 10 minutes per day, compared to an average of 34 minutes per day spent reading the newspaper (of course, the time spent watching television was probably for entertainment, rather than news; the comparison may thus be misleading). National Readership Study conducted in 1971 by Audits & Surveys, Inc., for the Newspaper Advertiser Bureau, as cited in Burns, op. cit.

[20]Report Concerning General Fairness Doctrine Obligations of Broadcast Licensees, 102 F.C.C. 2d 143 (1985); see also *Meredith Corp. v. FCC*, 55 U.S.L.W. 2391 (1987).

[21]*Report and Order*, 53 Rad. Reg. 2d (P&F) 1309 at 1324 (1983), as quoted in *Telecommunications Research and Action Center v. FCC*, 13 Med. L. Rptr. 1881, 1883 (D.C. Cir. 1986).

[22]*Sony v. Universal Studios, Inc.* 464 U.S. 417 (1984). Electronic publishing, also illustrates the way in which technology is overcoming time and space scarcity.

[23]47 U.S.C. 201-224 (1982).

generally liable for the content of the messages they transmit.

Drawing on the precedent of the postal system, the telegraph, and the railroads, the FCC defined communications common carriers as "any person engaged as a common carrier for hire."[24] This circularity causes a number of conceptual problems, particularly in questions of whether and how to regulate new media. The Supreme Court has defined common carrier in a less circular fashion, as "one who makes a public offering to provide [communications facilities] whereby all members of the public who choose to employ such facilities may communicate or transmit intelligence of their own design and choosing . . . ,"[25] but this does not solve the problem of when common carrier status may be mandated and imposed by the government.[26] The decision that a communication system is or is not a "common carrier" is a political rather than a technical decision. Legislatures tend to decide to regulate a system as a common carrier if it appears to have at least some of the characteristics of a natural monopoly.[27] Until recently, there has been no interaction between common carrier status and First Amendment concerns.[28] However, since the 1982 consent decree between AT&T and the Justice Department, AT&T has been denied the right to disseminate its own messages over its lines until 1989 because of the potential for anti-competitive behavior.[29] The

The First Amendment issues concerning the relationship between *media ownership* and control over the *content* that flows through that medium have been joined.

First Amendment issues concerning the relationship between *media ownership* and control over the *content* that flows through that medium have been joined. Among these issues are whether common carriers can also be publishers, who—as publishers—have the right to exclude other publishers from their fora; whether a monopoly common carrier can also do some publishing; and whether the government can compel some access over monopoly controlled facilities. The controversies over cable television and information services that might be available over telephone wires are illustrative of this issue, which promises to be the focal point of much First Amendment litigation for years to come.

[24]47 U.S.C. 153(h).

[25]*FCC v. Midwest Video Corp.*, 440 U.S. 689, 701 (1979).

[26]Broadcasters may not be treated as common carriers. 47 U.S.C. §153(h). Notwithstanding this, Direct Broadcast Satellite owners are permitted to choose between broadcast and common carrier type regulation. *National Association of Broadcasters v. FCC* 740 F.2d 1190 (D.C. Cir. 1984).

[27]"When 'natural' monopolies are recognized and entry is prohibited to all but the designated monopolist, the monopolist is normally required to provide universal service as a common carrier." Mark Nadel, "A Unified Theory of the First Amendment: Divorcing the Medium From the Message," *11 Fordham Urban Law Journal* 163, 193, n. 109 (1982). "The rate and service requirements imposed on these carriers under the Communications Act reflect the view that their natural monopoly status justifies government control of their business activities." Lynn Becker, "Electronic Publishing," op. cit., p. 855. See also *United States v. RCA*, 358 U.S. 334 (1959). Cable television was initially proposed as a candidate for common carrier regulation by the FCC, but the plan was abandoned.

[28]In the case of the telegraph, for example, the reason for the "dim perception [of First Amendment concerns] was that the early telegraph carried so few words at such a high cost that people thought of it not as a medium of expression but rather as a business machine. The computer suffered the same misperception a century later." Pool, *Technologies of Freedom*, op. cit., p. 91.

[29]Consent decree in *U.S. v. Western Electric*, 552 F.Supp. 131, 180-86 (D.C. Cir. 1982).

CABLE TELEVISION

When cable television entered the scene in the 1940s it was called Community Antenna Television (CATV), carried only existing broadcast channels, and was intended merely to provide better signals to homes in a bad reception area. Since that time, however, cable television has multiplied channel capacity manyfold. Systems that run two coaxial cables into the home can now provide up to 120 different channels. Initially, the FCC declined

jurisdiction over cable TV, but throughout the 1960s and 1970s, the Commission imposed a variety of access, content, and distant signal importation requirements. The Commission's authority to do so was based on the rationale that its regulations were "reasonably ancillary to . . . the Commission's various responsibilities for the regulation of television broadcasting,"[30] and broadcast television was "placed in jeopardy by the unregulated growth of CATV."[31]

Then, in the late 1970s and early 1980s, a series of Federal appeals court rulings struck down a variety of programming content regulations, based on either the First Amendment or statutory grounds.[32] Finding first that the FCC had failed to show that cable systems are "public forums" (i.e., common carriers), the language of one appeals court decision went on to frame the issue thus:

> The First Amendment rights of cable operators rise from the Constitution; the public's "right" to "get on television" stems from the Commission's desire to create that "right."[33]

In the Cable Communications Policy Act of 1984[34] Congress created such a right, albeit in limited fashion. It requires cable operators to provide "leased access channels" for commercial use "by persons unaffiliated with the [cable] operator,"[35] and it permits local franchising authorities to reserve public, educational, and government channels.[36] But cable operators take the position that because they do not suffer the physical limitations inherent in broadcasting, they are in the position of other publishers, and ought to have absolute editorial discretion. It seems likely, therefore, that even the limited content regulations set forth in the Cable Act will be challenged on First Amendment grounds.

But, as Ithiel de Sola Pool pointed out, "[the problem of access] may become the Achilles heel of what could otherwise be a medium of communication every bit as free as print."[37] Though many have argued that cable television is not a "natural monopoly," one cable franchise per municipality is nevertheless the rule and not the exception.[38] This suggests to some that cable operators ought to be treated in the same way as any other essential facility with substantial power to exclude others. Several commissions have come to this conclusion, but have still accepted the argument that treating cable as a common carrier would not provide adequate economic incentives for operators to build cable systems.[39] Even if cable systems are not treated as total common carriers, the question remains whether the government, to promote diversity, can require access to a certain portion of the available channels.

The delicate equilibrium that exists today between cable operators and television publishers will likely be disturbed as technology

[30] *U.S. v. Southwestern Cable Co.*, 392 U.S. 157 (1968)

[31] Ibid.

[32] For example, in *Home Box Office, Inc. v. FCC*, 567 F.2d 9 (D.C. Cir. 1977), overturned, on First Amendment grounds, rules restricting movies that could be shown over subscription television. In *Midwest Video Corp. v. FCC*, 440 U.S. 689 (1979) (Midwest Video II), the Supreme Court struck down Federal (though not necessarily state) cable access requirements as beyond FCC jurisdiction; if access rules could not be imposed on broadcasters, they could not be imposed on cable operators on an "ancillary to broadcasting" rationale. In 1985, the Court of Appeals for the D.C. Circuit decided that "must carry" rules, which required cable systems to carry local broadcast signals, were unconstitutional under the First Amendment. *Quincy Cable TV v. FCC*, 768 F.2d 1434 (D.C. Cir. 1985), cert denied, 106 S.Ct. 2889 (1986). The court suggested, moreover, that even if the "must carry" rules had furthered a significant governmental interest, they might nevertheless be contrary to the principle announced in *Miami Herald Co. v. Tornillo*, *dicta* of some portent for categorization of cable for First Amendment purposes.

[33] The language is from the appeals court ruling in Midwest Video II, *Midwest Video Corp. v. FCC*, 571 F.2d 1025, 1054 (D.C. Cir. 1978).

[34] 47 U.S.C. §§ 601-639, Public L. No. 98-549, 98th Cong. 2d sess., 98 Stat. 2779-2806, 1984.

[35] 47 U.S.C. §612

[36] 47 U.S.C. §611

[37] Ithiel de Sola Pool, *Technologies of Freedom* (Cambridge, MA: Belknap Press, 1983), p. 166.

[38] Cable is often called a "natural monopoly" because, as a practical matter, only one operator may use rights of way over poles or through conduits to connect with subscribers' houses. Where these physical limitations are not present, or where there is sufficient excess physical capacity, a cable operator may raise First Amendment objections. *Los Angeles v. Preferred Communications, Inc.*, 106 S.Ct. 2034, 54 U.S.L.W. 4542 (1986).

[39] Two early studies of the cable industry, the Sloan Foundation (On the Cable (New York: McGraw-Hill, 1971) and the Whitehead Report (Cabinet Committee on Cable Communications, *Cable—Report to the President* (Washington, DC: U.S. Government Printing Office, 1974). The Whitehead report reached the conclusion that when cable reached 50 percent penetration, it should change to carrier status.

again brings new interests into play. Although cable is today primarily an entertainment medium, it may not necessarily remain so. Because it is a "broadband" medium (meaning that it has capacity for handling high volumes of all sorts of electronic traffic), cable is a suitable carrier for computer data, electronic mail, videotex, databases, security monitoring, home banking and shopping, teleconferencing, and other interactive services. If cable systems are publishers under the First Amendment, and allowed to choose the content of what goes through their lines, they may well discriminate against content that is competitive to their own, or which do not yield as large a profit as entertainment products, such as Home Box Office (HBO) and other movie channels. In the future (perhaps the mid-1990s), fiber optic telephone connection to the home may make the telephone company a broadband highway for all information (with cable operators perhaps becoming customers of the telephone company), but for now, the tension between cable operators as First Amendment speakers and as forums for other would-be speakers will heighten.

The delicate equilibrium that exists today between cable operators and television publishers will likely be disturbed as technology again brings new interests into play.

INFORMATION SERVICES DELIVERED OVER TELEPHONE LINES

Technology has also blurred distinctions between computers and communications, between those who create a message (or data) and those who transmit it. This confounding of roles has raised First Amendment issues similar in kind to those raised by cable television; that is, how to reconcile the First Amendment interests of communications companies *as speakers* with the First Amendment interests of those *who seek access* to these companies' communications facilities. While the tension in the cable industry concerns whether cable operators will be required to grant a limited form of access to other would-be program providers, the issue here is whether telephone companies will be permitted to provide information services, using their own facilities, in competition with independent providers of the same or similar services.

Companies offering stock quotations, sports scores, airline schedules, and news retrieval services, among others, are concerned that the telephone companies could offer these same services themselves. Even more significant is the fear of the American Newspaper Publishers Association that telephone companies would provide electronic yellow pages and draw away a substantial chunk of newspapers' classified ads. Given the evidence of past discriminatory actions by AT&T against competitors, the modified final judgment (MFJ) settling the AT&T lawsuit barred the telephone company from entering the electronic publishing business.

The issue here is whether telephone companies will be permitted to provide information services, using their own facilities, in competition with independent providers of the same or similar services.

It is unclear whether the First Amendment permits such an absolute prohibition. Cable operators have been charged with discriminating by favoring their own affiliated pay networks over those of their competitors, yet they are not barred from carrying any of their own

services. One could argue that cable television systems are different from telephone companies because the former are not natural monopolies, but in *The Geodesic Network,*[40] a consulting report prepared for the Department of Justice, Peter Huber argued that local telephone companies are not natural monopolies either. He concluded that technology has changed the nature of communications from that of a hierarchical pyramid to that of a geodesic ring, so that the threat of dominance by one or a few industries is no longer possible.

Meanwhile, the FCC appears to believe that information services will not become widely available until the telephone companies offer information services. The agency, in its *Computer III* decision, argues that requiring all competitors to grant comparable efficient interconnection would be sufficient to ensure nondiscriminatory treatment.

[40]U.S. Department of Justice, Antitrust Division, *The Geodesic Network*, 1987 Report on Competition in the Telephone Industry, January 1987.

Part II

Scientific Communications and the First Amendment

Reconciling the maintenance of constitutional liberties with the requirements of national security poses an arduous challenge to democracy. Granted that a balance must be struck, where should the line be drawn? That is the puzzle for all who would presume to lead a free people. It implicates perhaps our most cherished contribution to social intercourse: Separation of Powers . . . . It is the undisputed responsibility of Congress and the Courts to maintain and regulate the right balance between measures necessary for the invulnerability of national security and the preservation of free expression.

—Martin L.C. Feldman, U.S. District Judge for the Eastern Division of Louisiana, Jan. 14, 1987

Chapter 4

National Security and Scientific Communications

SCIENCE, FREE SPEECH, AND NATIONAL SECURITY

Science and technology were recognized by the Founding Fathers as indispensable to the "common Defense and general Welfare."

The U.S. Constitution empowers Congress to regulate commerce, to fix the standard of weights and measures, to establish post offices and post roads, and to secure for authors and inventors the exclusive right to their respective writings and discoveries in order to "promote the Progress of Science and useful Arts."[1]

There is nothing else in the Constitution directly related to science and technology. It was assumed that the States would have primary responsibility for the useful arts such as agriculture, manufacturing, construction, and medicine. But the few provisions in Article I are significant, because they clearly indicate that science and technology were recognized by the Founding Fathers as indispensable to the "common Defense and general Welfare" and an appropriate subject of attention and support for Congress.

The men who wrote the Constitution were well educated in the science of their day and enthusiastic about advances in technology. James Madison avidly studied and wrote about natural history and agriculture science. Benjamin Franklin was one of the world's leading scientists. Hamilton studied medicine, chemistry, and mathematics.

[1]Article 1, Sec. 8 also provides authority for Congress to "make all Laws which shall be necessary and proper for carrying into Execution" these and other powers derived from the Constitution.

Scientific activity or communications have not in practice enjoyed the special status given political comment.

They understood well the importance of scientific freedom, as is shown by their writings. But even with the addition of the first Ten Amendments to the Constitution, in 1791, scientific freedom was not singled out for special protection; it was presumed to be included with other areas—politics, religion, philosophy, economics—in the broad protections given to speech, publication, assembly or association, exercise of religion, petition and protest, all included within the First Amendment.[2]

None of these First Amendment protections is absolute under prevailing constitutional doctrine. There are times and conditions when the interests of the Nation as a whole override the right of the individual to say and do as he or she wishes. Both Congress and the Supreme Court have treated political speech as that speech most strongly protected by the First Amendment. Commercial speech—that is, advertising—is least protected; and may be regulated as to time, place, and manner.[3]

Scientific activity or communications have not in practice enjoyed the special status given political comment, although some constitu-

[2]Steven Goldberg, "The Constitutional Status of American Science," *University of Illinois Law Forum*, vol. 1979, No. 1, 1979. pp. 1-6ff.

[3]Before *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc.*, in 1976, the Supreme Court did not treat commercial speech as protected speech; it was fully subject to State police power. The extent of, or limits on, protection for commercial speech are somewhat uncertain at this time.

Is there a potential constitutional conflict between the rights of free speech and press guaranteed by the First Amendment, and government restrictions on the communication of scientific information in the interest of national security?

tional scholars argue that this was the clear intent of the First Amendment separation of church and state.[4] It is not, indeed, clearly established that there is "a right to do research," nor have the limits of governmental authority to restrict speech and press (publication) in the area of science and technology been clearly defined, by either Congress or the Courts.

Representative George Brown, in 1982, warned Congress:

> Recent administration actions . . . sharpen the conflict between constitutional protections and the requirements of national security. . . . The issues at stake stem from the conflicting demands of the most fundamental matters in national policy: the security of the Nation and its economic well-being, versus the rights of citizens to privacy, assembly, free speech, travel, and freedom from unwarranted Government interventions.[5]

Is there a potential constitutional conflict between the rights of free speech and press guaranteed by the First Amendment, and government restrictions on the communication of scientific information in the interest of national security? Is the balance between these two interests—both of critical importance to American constitutional government—being maintained, or is it endangered?

A fundamental tenet of scientific methodology is that basic scientific research results or new scientific theories should be published,

[4]Goldberg, op. cit., says that the Founding Fathers, as "men of the Enlightenment," saw established churches as having been the enemy of free scientific investigation.

[5]*Congressional Record*, vol. 128, No. 16, Feb. 25, 1982, p. H511.

One issue addressed in this report is the extent to which national security and foreign trade interests have converged and perhaps in some respects may even have been confused.

widely disseminated, and thoroughly argued, and the results replicated. In part this is in order to share knowledge with other scientists for the ultimate benefit of people in general. More immediately, it provides a test and means of validation.

> Science gets at the truth by a continuous process of self-examination which remedies omissions and corrects errors. The process requires free disclosure of results, general dissemination of findings, interpretations, conclusions, and widespread verification and criticism of results and conclusions.[6]

The First Amendment

The Supreme Court has recognized in numerous cases that Congress (or State legislatures) may make laws that limit freedom of speech or press. Government must, however, sustain a substantial burden of proof to justify an interference with speech or press. As a general rule, expression may not be restricted because of its content, although some categories of expression are given less protection than others.[7] Government restrictions on free speech may however be valid under a "balancing of interests test" when those restrictions are incidental to legitimate government purposes not directly related to speech or press.[8]

The protection of freedom of speech and freedom of press is therefore not absolute. Many

[6]Harold C. Relyea (ed.), "Shrouding the Endless Frontier—Scientific Communication and National Security: The Search for Balance," *Striking a Balance: National Security and Scientific Freedom* (Washington, DC: American Association for the Advancement of Science, 1985), p. 76.

[7]*Police Department of Chicago v. Mosely*, 408 U.S. 92 (1972). "Fighting Words" and obscenity are generally not protected.

[8]*Adderly* v. *Florida*, 385 U.S. 39 (1966); *Brown v. Louisiana*, 383 U.S. 131 (1966); *Kovacks v. Cooper*, 336 U.S. 77 (1949); *Breard v. Alexandria*, 341 U.S. 622 (1951); *O'Brien v. United States*, 391 367 (1968).

restrictions are placed on scientific communication in the interests of national security. National security may be defined as the military, defense, and foreign relations objectives of this Nation. This definition has implicitly been broadened over time to include protection of economic and trade objectives. One issue addressed in this report is the extent to which national security and foreign trade interests have converged and perhaps in some respects may even have been confused.

Where government action involves a "prior restraint," that is, a prohibition prior to rather than a punishment after the communication, the constitutional test is much more severe. There is a "heavy presumption" against the constitutional validity of any prior restraint.[9] The seminal Supreme Court decision is *Near v. Minnesota* where it was held that with certain limited exceptions prior restraints were constitutionally impermissible.[10]

Threats to national security can make it necessary to limit free speech. The court ruled in *Schenck v. United States*,[11] that impingement on freedom of speech in certain circumstances "appears to be a reasonable exercise of sovereign power . . . in the interest of the common defense and security."

In recent years not only has scientific exchange or publication been limited in the interest of national security, but it arguably has also been limited in the interest of national trade balances. Thus the question: As we enter the third century of constitutional government, have these restrictions taken together burdened the exercise of free speech and press to a degree that may violate the First Amendment, and by so doing threatened the future advancement of science and technology?

[9]*Bantam Books v. Sullivan*, 372 U.S. 58, 70 (1973); *Vance v. Universal Amusement Co.*, 445 U.S. 308, 317 (1980); *Organization for a Better Austin v. Keefe*, 402 U.S. 415, 419 (1971).

[10]293 U.S. 697 (1931). Exceptions for example include obstruction of military recruiting, publication of the sailing dates of military transports or of the number and location of troops; publication of obscene matter, and incitements to violent or forcible overthrow of the government.

[11]249 U.S. 47 (1919).

The real question is whether *taken together, the effects of these restrictions place a limitation on scientific freedom so as to contravene the intent of the First Amendment.*

What Activities Are Restricted and How?

Scientific information includes not only publishing in professional journals or the public media, but also:

- presentation of papers or giving of lectures in professional meetings or other fora,
- distribution of unpublished papers or reports,
- participation in workshops or working sessions,
- discussions among colleagues, and
- classroom or laboratory instruction.

These activities have been restricted in the interest of national security:

- under Executive Orders;
- by or under legislation, including:
  - —the Atomic Energy Act,
  - —the Invention Secrecy Act, and
  - —Export Administration and Arms Export Control Acts;
- by contractual agreement between researchers and government agencies; or
- by self-restraint agreements of researchers and professional societies.

Each of these means is to be considered in the context of judicial precedents as to their constitutional standing. However, as already noted, the real question is whether *taken together, the effects of these restrictions place a limitation on scientific freedom so as to contravene the intent of the First Amendment and its declaration of the rights of free speech and press.*

The Background of the Issue

At least since World War II, it has been generally accepted that national security requires

After the war, the growing centrality of science-based technology both for industry and for national defense was clear.

that secrecy be imposed on some research. Government has been able without serious challenge to restrict dissemination or results of research conducted by Federal employees, even in peacetime. Beginning in 1940, a series of Executive Orders established criteria and classifications for assuring the secrecy of government documents. The first War Powers Act, immediately after Pearl Harbor, also gave the President the power to censor all communications with foreign countries.[12] Later this power to censor direct communications across national borders was expanded to encompass publication of information that would prejudice our military/defensive interests or aid an enemy.

There has been only slightly more questioning of restrictions on the dissemination of research paid for by the Federal Government but done in universities and other nongovernment institutions. Scientists have also voluntarily withheld scientific information in the interest of national security. Even before the United States entered the Second World War, a special committee of the National Research Council, working cooperatively with editors of professional journals, reviewed papers for possible defense-related information that should not be published. This self-restraint, it should be emphasized, applied to information with a clear tie to offensive or defensive weapons.

The Federal Government exercised tight security over scientific research during the war, most notably over the Manhattan Project and other activities related to development of atomic weapons. After the war, the growing centrality of science-based technology both for industry and for national defense was clear. As political tension grew between the Western allies and the Soviet bloc countries, there were early signs that traditional assumptions about science and the First Amendment would be challenged. In 1948, scientist and statesman Vannevar Bush noted that:

> . . . the critical point [where fundamental science gives rise to applications] may well be reached far earlier in the process than we are accustomed to think, and . . . we must be alert to it and ready at once to erect the defenses of protection and security which it demands.[13]

Even during the 1940s other leading scientists complained about excessive secrecy. They argued that restricting access to scientific knowledge might do more harm than good for America's continued leadership in science and technology. Determined collection of information by hostile nations can seldom be effectively blocked, they said, but internal flows of ideas and research results may be unintentionally obstructed.

By the mid-1970s, there was strong concern over international competitiveness in both world markets and domestic markets. The United States was no longer the unquestioned leader in all areas of advanced science and technology, as it had been in the 1950s and 1960s. Increasingly, scientific leadership translates directly into military advantage. Thus trade and technology policy clearly overlaps national security policy. Congressman Don Bonker, chairman of both the House Foreign Affairs Subcommittee on International Economic Policy and Trade and the House Export Task Force in 1986, says flatly:

> Our defense strategy rests on qualitative technical superiority over the Warsaw Pact countries, and we must insure that the Western alliance maintains this technological edge.[14]

[12]U.S. Congress, Office of Technology Assessment, *The Regulatory Environment for Science—A Technical Memorandum*, OTA-TM-SET-34 (Washington, DC: U.S. Government Printing Office, February 1986).

[13]U.S. Congress, House Committee on Government Operations, "Availability of Information From Federal Departments and Agencies, Part 8," *Hearings*, 85th Cong., 1st sess., Washington, DC, pp. 2159-2160.

[14]Don Bonker, "Protecting Economic Interests," *Issues in Science and Technology*, fall 1986, p. 97.

The boundary between traditional categories of "basic" and "applied" research has blurred, making it harder to restrict only the latter.

The tension between scientific free speech and national security protections has become increasingly troublesome in this decade. One reason is that there has been a significant expansion in the meaning of national security. The term no longer applies merely to direct military threat. It also means the long-term risks of change in the military, economic, and political balance of power between nations. To this balance, relative scientific and technological capabilities are deemed critical.

Many or even most areas of advanced industrial technology have potential military applications. Most nations potentially hostile to the United States and its allies make no real distinctions between government, military, and scientific institutions. Any data exchanged between U.S. scientists and scientists of those nations has also been communicated to and between government institutions of those countries.

The scope of national security restrictions has been significantly broadened in the past decade. These restrictions apply to a growing proportion of scientific activity. The high cost of research at the leading edge of science and technology has led to more of it coming from government funding. A growing proportion of that funding comes from the Department of Defense (DoD).[15] The boundary between traditional categories of "basic" and "applied" research has blurred, making it harder to restrict only the latter. There is interdependency between government research and that done in universities and independent laboratories even without government funding.

DoD statements about national security restrictions on scientific communications are sometimes misunderstood by the unwary because of the tendency of many DoD officials to make a sharp, but sometimes unspoken, distinction between "scientific information" and "technical data," to associate the former only with "fundamental research," which by DoD definition is unrestricted, and to associate the latter with applied research and development, or with technology. Thus "scientific information" is by a truism, unrestricted. With regard to most areas of advanced scientific research, and particularly those that have to do with computers and communications technologies, it is increasingly difficult to understand, to defend, or to make such a distinction between scientific information and technical data.

[15]The Federal Government supported about 48 percent of all R&D in the United States in 1986 (industry support accounts for another 48 percent). The average annual rate of growth in constant dollars is 5.9 percent for all R&D spending, 5.8 percent for industry, and 7.3 percent for the Federal Government. DoD's R&D obligations increased by 13 percent annually from 1982 to 1986, and by 20.9 percent for 1986 to 1987. Government provided 63 percent of funding for academic research in 1986. Defense R&D in 1986 probably accounted for 73 percent of all Federal R&D support. National Science Foundation, *Science and Technology Data Book*, NSA 86-311 (Washington, DC: National Science Foundation, 1986).

THE EXECUTIVE BRANCH AND CLASSIFICATION OF DOCUMENTS

The classification of information, in categories ranging from "confidential" up through increasingly stringent classes of "secret" and "top secret,"[16] is done under a series of Presidential Executive Orders. It is intended to apply to information that would create or increase

[16]Within the Secret and Top Secret categories there are many "compartments" or "special access programs" or subcategories to further restrict access to information to those with a need to know, defined with appropriately varying degrees of rigor. These special access programs may be set up by designated agency heads (primarily DoD, the intelligence agencies, and the Department of Energy [DOE]) to provide greater protection for certain kinds of information or to conceal the means and channels through which information is acquired, or for similar reasons. See Sec. 4.2 of Executive Order 12356, Apr. 2, 1982. Access to restricted information defined by the Atomic Energy Act, as described later, is governed by DOE's Q Clearance and is also compartmentalized.

a military risk to the United States or prejudice its foreign policy objectives. The President, as Commander-in-Chief, is considered to have full authority to classify information generated by the government.

In 1970, a Defense Science Board task force concluded that too many documents were classified.[17] It recommended revision of the security classification process to declassify as much as 90 percent of classified information. As a general rule, the task force said, basic research should never be classified. Even "confidential" or special access limitations were inappropriate for basic research and likely to seriously impede technical programs. Security is most essential for information at the applied end of the spectrum, that is, close to design and production. Throughout the 1960s and most of the 1970s, the trend was toward classifying less material.[18]

Executive Order 12356 and the Corson Panel

Executive Order 12356,[19] issued in April 1982, reversed a 30-year trend toward narrowing the scope of classification and the discretion of bureaucrats in assigning secrecy classifications.[20] It eliminated an explicit provision, which appeared in earlier classification orders, forbidding classification of information in which the government has not acquired a property interest. It lowered a standard, adopted in 1978, that required an identifiable harm to national security from disclosure. It added two new categories, for cryptology and for information bearing on systems vulnerability.[21] The order instructed classifiers, when in doubt, to err on the side of classification,[22] whereas the policy of several preceding Administrations had been to lean toward not classifying or toward a lower classification. For these reasons, and because the order had been developed in a particularly closed and secretive manner, it was widely criticized in Congress.[23]

Many researchers argue that the possibility of classification has a strong "chilling effect" on scientific communications in general.

The number of decisions made in one year to classify documents probably hit an all-time peak in 1982 of over 1 million. By comparison there were approximately 900,000 new classifications in 1985.[24] In the Department of Defense, 2,300 officials now have the authority to make classification decisions.[25] The total volume of classified documents is huge and growing rapidly.

Most of these are not from university-generated information. A DoD study in 1984 sur-

[17]U.S. Department of Defense, *Report of the Defense Board Task Force on Secrecy* (Washington, DC: July 1970).

[18]Harold C. Relyea, *National Security Controls and Scientific Information*, Congressional Research Service Issue Brief B82083, updated June 17, 1986, p. 6.

[19]47 Fed. Reg. 14874-14884 (Apr. 6, 1982).

[20]Harold C. Relyea, *National Security Controls and Scientific Information*, Congressional Research Service Issue Brief B82083, updated June 17, 1986, p. 6.

[21]These categories were listed explicitly in Executive Order 12356; some national security experts had argued for some time that such information was implicitly subject to classification.

[22]Sec. 1.1 (c) says: If there is reasonable doubt about the need to classify information it shall be safeguarded as if it were classified pending a determination by an original classification authority, who shall make this determination within thirty (30) days. If there is reasonable doubt about the appropriate level of classification, it shall be safeguarded at the higher level of classification pending a determination by an original classification authority, who shall make this determination within thirty (30) days.

[23]U.S. Congress, House of Representatives, Committee on Government Operations, *Executive Order on Security Classification, Hearings*, 97th Cong., 2d sess., Mar. 10 and May 5, 1982. Also House Report 97-731. Representative Glenn English, Chairman of a House Subcommittee on Government Information and Individual Rights, said, "The basic message to bureaucrats would be: When in doubt, classify." Morton Halperin, director of the Center for National Security Studies, said that the order would eliminate key provisions intended to prevent national security concerns from encroaching on scientific research.

[24]According to Steven Garfinkel, the chief of the U.S. Information Security Oversight Office, in a talk at the annual meeting of the American Association for the Advancement of Science, Feb. 18, 1987, as reported in *The Institute*, a publication of the Institute of Electrical and Electronic Engineers, Inc., vol. 11, No. 4, April 1987, p. 1.

[25]The count was made by the Security Review Commission, a group created by the Secretary of Defense in 1985 and headed by General Richard G. Stilwell; according to information provided to OTA by the Office of the Secretary of Defense, May 7, 1987, citing S.F.311. For further discussion see "Espionage and Security Leaks: Diagnosis and Therapy," by Harold P. Green, of the National Law Center and the Graduate Institute for Policy Education and Research, The George Washington University, 1986.

veyed over 123,000 DoD research reports. Only 19 percent came from university researchers; 3.5 percent of these fell under distribution limitations, and only 1.3 percent were classified.[26] Many universities will not do classified research, which explains the low volume. Some, however, do permit classified research if approved by the school's administration. An unknown number of papers are probably "sanitized" before publication, and many researchers argue that the possibility of classification has a strong "chilling effect" on scientific communications in general.

A special panel of the National Academy's Committee on Science, Engineering, and Public Policy was formed in 1982, before Executive Order 12356, at the request of DoD and intelligence agencies. The panel, chaired by Dale R. Corson, president emeritus of Cornell University, conceded that there had been much "involuntary technology transfer" from the United States to potentially hostile countries. But the panel also said that relatively little of the deleterious leakage came from universities or from open scientific literature.

The panel recommended that there be no restrictions limiting access to any area of university-performed basic or applied research, unless:

- the area is developing rapidly, and the time from basic science to application is short;
- the information has identifiable, direct military applications or is dual-use, involving process and production techniques;
- the information would give the U.S.S.R. a significant near-term military benefit; and
- the United States, or other friendly nations with secure control systems, is the only source of the information.

[26]Mitchel B. Wallerstein and Lawrence E. McCray, "Scientific Communication and National Security: Issues in 1984," *NAS News Report* (Washington, DC: National Academy of Sciences, April 1984). The study did not say what proportion of university research is restricted.

The power of government to protect State and military secrets has always been regarded as inherent and fundamental.

Information that meets *all* of these criteria should be classified. But since most universities will not do classified research, the Panel recommended as an alternative, written agreements between the university and the government that (a) prohibit participation by nationals of some foreign countries in such research, and (b) require pre-publication review of articles by the Federal agency.

DoD concluded that the Corson panel criteria were "too difficult to translate into operational considerations" and decided simply to "retain its black/white policy towards university research—i.e., if not classified, then no restriction."[27]

The present Administration continues to emphasize classification of government documents. It has, in addition, made increasingly explicit and forceful use of other means of restricting scientific communication.

The Authority for Presidential Classification of Documents

The power of government to protect State and military secrets has always been regarded as inherent and fundamental. Although military and State secrets have been protected in the United States at least from the time of Washington's Presidency, there is little clear statutory authority, aside from the atomic energy area, for classification of information.[28] The closest approach to a statutory basis is probably Section 161 of Revised Stat-

[27]The quotations are from a review of an OTA draft of this report by officials in the Office of the Secretary of Defense, May 1987.

[28]*Constitutional Implications of Federal Restrictions on Scientific Research and Communication*, March 1987, by Harold P. Green, The George Washington University National Law Center, Washington, DC.

utes,[29] dating back to the early days of the Republic. As originally written, it authorizes the head of each government department:

> . . . to prescribe regulations . . . for the distribution and performance of its business, and the custody, uses, and preservation of the records, papers, and property appertaining to it.

The basic authority for classification of information has been the President via a series of Executive Orders—not grounded on explicit statutory authority but on the authority vested in the President by the Constitution and laws of the United States. The first of these Executive Orders was No. 10290, promulgated by President Truman in 1951, which limited "classified information" to "official information,"[30] assumed to be information in which the government has some kind of proprietary interest. In President Eisenhower's Executive Order 10501,[31] use of the word "official" again connoted that classification was limited to information that in some way belonged to the government. President Carter's revision, in Executive Order 12065,[32] made this explicit by specifying that a product of nongovernment research and development accomplished without access to classified information was not subject to classification "until and unless the government acquires a proprietary interest. . . ."

President Reagan's Executive Order 12356,[33] however, includes no such limitation, but brings within its ambit any information that "is owned by, produced by, produced for, *or is under the control of* the United States Government" (emphasis added). This provides some "color of authority" for classification of information that is privately developed without any involvement or funding by the government.[34]

[29]Subsequently incorporated into 5 U.S.C. 22; and since 1966 found at Sec. 301 of Title 5.

[30]16 Fed. Reg. 9795, et seq. (Sept. 27, 1951).

[31]18 Fed. Reg. 7049, et seq. (Nov. 10, 1953).

[32]47 Fed. Reg. 14874, et seq. (Apr. 6, 1982).

[33]47 Fed. Reg. 14874, Sec. 6.1(b)

[34]These Executive Orders all provide that authority under the Atomic Energy Act pertaining to Security regulation of private information (discussed below) is not affected by Executive Orders.

The Atomic Energy Act of 1946 added a new concept to traditional classification procedures—the idea that some information was "born classified."

Troubling First Amendment issues are presented if government attempts to restrict the freedom of scientists to do independent, private research or to communicate information that is privately generated. Except in the area of atomic energy, however, the government has not generally attempted to extend classification to scientific endeavors conducted without government involvement, although recent actions to be described below have introduced some uncertainty about this policy.

The Congress and Legislated Secrecy

The Atomic Energy Act

The Atomic Energy Act of 1946, modified in 1954,[35] added a new concept to traditional classification procedures—the idea that some information was "born classified." The 1946 Act included provisions, frankly headed "Control of Information,"[36] which established a category of information called "Restricted Data," defined to mean " . . . all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy . . . ;" except when such data has been expressly declassified. Misuse of Restricted Data was subject to heavy criminal penalties that paralleled the more universal provisions of the Espionage Act.[37]

[35]The 1954 Act, 68 Stat. 919; 42 U.S.C. 2011-2296, relaxed the provisions of the 1946 Act in some regards to allow private sector development of atomic energy.

[36]42 U.S.C. 2004 (y). The Atomic Energy Commission (AEC) was given explicit authority to promulgate regulations and issue orders for the protection of Restricted Data. The Act required, or at least was interpreted as requiring, that no person could be given access to Restricted Data without a prescribed investigation into his/her character, associations, and loyalty on the basis of which Security clearance was to be granted.

[37]42 U.S.C. 2275-2277. Unlike the situation with respect to ordinary classified information, there is an explicit nexus between Restricted Data and those special espionage-type provisions.

A provision of the Act authorized the issuance of court injunctions to restrain any threatened violation of any provisions of the Act or its implementing rules or regulations. Since the injunction provision was applicable to the information control provisions, it can be read as encompassing prior restraints on the communication of Restricted Data.

These provisions are unique in a number of respects. No other Federal statute has ever purported to control information in this way. The definition of Restricted Data is extremely broad and could embrace a great deal of information contained in conventional textbooks on physics and chemistry. Normally, classification of information requires an affirmative determination that it needs security protection, but Restricted Data is "born classified"[38] if it falls within the statutory definition. While ordinary classified information (at least until issuance of President Reagan's Executive Order) has always been limited to "official" information, the definition of Restricted Data includes "all" data, thereby raising the question of whether it includes data generated wholly in the private sector without any government support or involvement.[39]

The answer to this question is not entirely clear. Legal arguments can be constructed for both positions. Under the Atomic Energy Act of 1954, Congress accepted at least implicitly the proposition that Restricted Data included some data generated wholly outside the government, since one provision of the Act explicitly treats information developed in other countries as Restricted Data.[40]

Moreover, the authors of the 1946 Act seem to have intended that the information controls extend to privately developed information; Senate staff members who played a major role in drafting the 1946 Act[41] later wrote:

> It does not matter whether these (Restricted) data are discovered or compiled in a government laboratory or in connection with the private research of an individual scientist.

On July 21, 1947, the Attorney General wrote the Chairman of the Atomic Energy Commission (AEC) stating that there was "considerable indication" that Congress meant the information control provision of the Act to apply to nongovernment information, but recommending a "simple amendment" of the Act to remove any doubt.[42]

Nevertheless, there is no statutory provision that *explicitly* authorizes restrictions on privately developed information. Some experts hold that merely inferring such authority from statutory provisions would not pass constitutional muster.[43]

The AEC and its successors, the Energy Research and Development Administration (ERDA) and later the Department of Energy (DOE), have proceeded on the assumption that privately developed information is subject to the full array of controls.[44] The information control provisions have been invoked for regulatory purposes—such as retarding activities in the United States that could lead to proliferation of nuclear weapons in other countries.[45]

[38]Richard Hewlett, " 'Born Classified' in the AEC: A Historian's View," and Harold Green, "A Legal Perspective," *Bulletin of Atomic Scientists*, December 1981, pp. 20-27 and 28-30.

[39]One provision, 42 U.S.C. 2201(i), authorizes regulations "to protect Restricted Data received by any person in connection with any activity authorized pursuant to this Act." This is probably not sufficiently broad to reach privately generated information. Another provision, 42 U.S.C. 2201(p) authorizes regulations "necessary to carry out the purposes of this Act." It is this latter authority that the AEC relied on for the proposed Part 26, to be discussed.

[40]42 U.S.C. 2162(e).

[41]J. Newman and B. Miller, *The Control of Atomic Energy*, (New York: Whittlesey House, 1948), p. 15 ff. Newman and Miller were on the staff of the Senate Special Committee on Atomic Energy when the Act was drafted. Newman and Miller wrote, ". . . if the Act does not restrict the liberty of scientific thought, it without question, abridges freedom of scientific communication. The controls on information were deliberately designed to regulate the interchange of scientific ideas . . ." (p. 208).

[42]According to Professor Harold P. Green, of the George Washington University National Law Center; documentation is available in Department of Energy Archives.

[43]*Greene v. McElroy*, 360 U.S. 474, at 506-608 (1959).

[44]Draft memorandum, "Authority To Control Dissemination of Privately-Developed Restricted Data," Feb. 28, 1966, from Franklin N. Parks, AEC Assistant General Counsel, to Joseph F. Hennessey, AEC General Counsel, available in DOE Archives.

[45]Richard Hewlett, " 'Born Classified' in the AEC: A Historian's View," *Bulletin of Atomic Scientists*, December 1981, p. 22.

The AEC on several occasions declared wholly private scientific information to be Restricted Data.

In congressional hearings in 1955,[46] the AEC General Counsel asserted that a scientist working in his own laboratory, with no government connection, could be compelled to submit to AEC security requirements, including classification and personal clearance, if he was creating data that would be regarded as Restricted Data if created in an AEC facility.

The AEC on several occasions declared wholly private scientific information to be Restricted Data.[47] In these cases the applicability of atomic energy information control provisions has affected primarily profit-seeking business organizations rather than universities. Although in each case the affected company sustained real economic injury, there has been only one judicial challenge. The corporations apparently concluded that private business interests would not prevail in court over government's national security claim.

In the only case in which a court has considered the constitutional issue,[48] the Court of Claims rejected a contention that the classification of an industry process was a "taking of property" entitling the corporation to just compensation under the Fifth Amendment.

[46]*Hearings on S. J. Res. 21 to Establish a Commission on Government Security*, Subcommittee on Reorganization, Senate Committee on Government Operations, 84th Cong., 1st sess. (1955), pp. 240-241, 267-271.

[47]Richard Hewlett, " 'Born Classified' in the AEC: A Historian's View," and Harold Green, "A Legal Perspective," *Bulletin of Atomic Scientists*, December 1981, pp. 22, 27 and 29. One example involved a corporation attempting to use gas centrifuge technology for separating uranium isotopes. The most explicit assertion by the AEC of the right to control private information came in 1967, when the AEC proposed a new regulation, Part 26, dealing with "Private Restricted Data," whereby in effect private research and development in the fields of nuclear explosives and gas centrifuge technology for producing nuclear fuel, was totally prohibited. Eventually, this AEC proposal was withdrawn. Proposed 10 CFR Part 26, App. A, 32 Fed. Reg. 6707.

[48]*Radioptics, Inc. v. United States*, 621 F. 2d 1113,223 Ct. Cl. 594 (1980).

Where government action involves a "prior restraint" on communication, the constitutional test is most severe.

The Court said that classification did not absolutely prohibit the plaintiff's use of the concept but only regulated its use, and was thus not a taking. Further, when the purpose of a regulation is to prevent injury to the public, compensation is generally not constitutionally required.

The Federal Government bases the restriction of privately generated information on the *Schenck v. United States*[49] finding that impingement on freedom of speech "would appear to be a reasonable exercise of sovereign power . . . in the interest of the common defense and security."[50] The provisions of the Atomic Energy Act taken together seem to authorize a Federal court to issue an injunction restraining a defendant's communication or publication of even privately developed information, which would be prior restraint.[51] Is this authority constitutional?

As already noted, where government action involves a "prior restraint" on communication, the constitutional test is most severe. The government sought an injunction to restrain publication of the Pentagon Papers by *The New York Times* and *The Washington Post*. In *The New York Times Co. v. United States*,[52] the Supreme Court held in a 6-3 decision that this burden was not met.

In 1950, the AEC ordered *Scientific American* not to publish, without specified deletions,

[49]249 U.S. 47 (1919).

[50]According to Richard Hewlett, " 'Born Classified' in the AEC: A Historian's View," *Bulletin of Atomic Scientists*, December 1981, pp. 23-25. Hewlett notes that this reasoning was plied to AEC's proposed "Part 26" (see footnote above) in 1966. The Atomic Energy Committee of the Bar of the City of New York sent the AEC a detailed brief challenging the constitutionality of the proposed rule.

[51]Such an injunction was in fact issued in the *Progressive* case, to be discussed. 467 F. Supp. 990 (W.D. Wisc. 1979).

[52]403 U.S. 713 (1971).

an article on thermonuclear weapons. The article, which had already gone to press, was by Dr. Hans Bethe, an eminent theoretical physicist long involved in the nuclear weapons program. The publisher protested that all of the technical information in the article "was well known to physicists . . . and had been widely published." The AEC insisted that Bethe's authorship confirmed the authenticity of previously published information. *Scientific American* capitulated under the AEC's threat to seek an injunction, and AEC security officers supervised the destruction of the type and plates and the burning of 3,000 copies of that issue.[53]

Until 1979, 33 years after the enactment of these information control provisions, there was no litigation challenging the constitutional validity of prior restraint on publication of Restricted Data. *United States v. The Progressive* (1979)[54] made a weak case for the challenge. *The Progressive* proposed to publish an article[55] in which a journalist purported to describe how hydrogen bombs are made and work. The intent was to alert the public to the "false illusion of secrecy" created by the government and the necessity for decisive action to halt the proliferation of nuclear weapons. The information was derived entirely from the public domain. The government held that:

> When drawn together, synthesized and collated, such information acquires the character of presenting immediate, direct, and irreparable harm to the interests of the United States.

The court found "no plausible reason why the public needs to know the technical details about hydrogen bomb construction to carry on an informed debate" on the issue of proliferation. With respect to prior restraint, the court returned to *Near v. Minnesota*, in which the Supreme Court had spelled out certain situations in which restraints on expression might be constitutionally permissible; and said that publication of technical information on the hydrogen bomb was "analogous to publication of troop movements or locations in time of war," thereby falling within the "extremely narrow exception to the rule against prior restraint."[56]

The decision was never subjected to review by higher courts, since it was mooted by publication of essentially the same information in another journal. According to Congressman George Brown:[57]

> . . . [because] the Supreme Court had ruled in the Pentagon Papers case that prior restraint was not tenable, it is not clear what would have happened to the *The Progressive* case if it had been reviewed by the Supreme Court.

Professor Harold Green of the National Law Center says:

> [T]he case stands as vivid testimony to the potential impact on scientific freedom of the information control provisions of the Atomic Energy Act.

The Invention Secrecy Act

The Invention Secrecy Act passed in 1951[58] allows the Federal Government (through the Commissioner of Patents) to block the granting of a patent or the disclosure of technological information by an inventor, when this disclosure "would be detrimental to national security," even where the government has no property interest or right in the invention.[59] In the 1970s the National Security Agency (NSA), for example, frequently asked for "secrecy orders" for cryptographic inventions, but this decreased sharply in the late 1970s

[53] *Scientific American*, May 1950, p. 26.

[54] 467 F. Supp. 990 (W.D. Wisc. 1979).

[55] The article, not published, was Howard Morland, "The H-Bomb Secret: How We Got It, Why We're Telling It."

[56] *United States v. The Progressive, Inc.*, 467 F. Supp. 990 (W.D. Wisc. 1979), 996.

[57] *Congressional Record*, vol. 128, No. 16, Feb. 25, 1982, H511.

[58] Invention Secrecy Act of 1952 (35 U.S.C. 181-188).

[59] There are two categories of inventions subject to this act. In the first, government has a property interest, and the invention is therefore already subject to classification; in the second, government does not have a property interest. Patent officials estimate that roughly 4,800 inventions are the subject of invention secrecy orders at any one time; that about 1,000 of them are foreign inventions covered under reciprocal agreements with various friendly nations; and that of the remainder, approximately 20 percent fall into the second (nongovernmental property interest) category.

when the procedures for requesting secrecy orders were changed and made more rigorous.

Secrecy orders are effective for only one year, but may be renewed. However, although this limitation was written into the Invention Secrecy Act when it was passed in 1951, for the next 27 years it was inapplicable. The law contained an "exception" clause to the effect that the yearly renewal requirement was not operative for the duration of a war or national emergency, and for some months thereafter; and the National Emergency proclaimed during the Korean War was not officially terminated until 1978. The annual renewal cycle has been in effect since that time, but has been protested by national security officials, at least as it applies to inventions already subject to periodic reexamination for classification downgrading (i.e., those in which government has a property interest).

Many secrecy orders are issued in connection with already classified patent applications. Sometimes, however, the patent application has been filed by persons who developed the invention without any government involvement.

In February 1987 the Army requested and the Patents Commissioner granted a secrecy order on an application for an American patent in the field of "zero-knowledge proofs," by an Israeli mathematician, working in an Israeli institute.[60] While such proofs are used in cryptology, they are generally regarded as advances in theoretical or "pure" science. The applicant was ordered to "recover and destroy" all related materials. The secrecy order was quickly withdrawn, since the government cannot classify work done by foreigners in their own country, but not before there were many protests from mathematicians. This episode was taken to indicate that American achievements of the same kind might be restricted.

The constitutionality of the Invention Secrecy Act has never been tested. Since the grant of a patent secures a property right conferred by the government, a patent applicant is subject to the conditions established by the government. Some experts have held that constitutional objections are further obviated by the statutory requirement that the patent applicant receive just compensation for any loss that might be suffered by reason of the secrecy order.

The constitutionality of the Invention Secrecy Act has never been tested.

However, a House of Representatives Report in 1980[61] noted that:

> No secrecy order ever underwent judicial review for appropriateness. There has been no First Amendment judicial test of the Invention Secrecy Act, and the statutory right of an inventor to just compensation for secrecy order damages appears more illusionary than real.

The report noted that from 1945 to 1980 there had been 29 claims for compensation, one claim for every 1,000 secrecy orders; 6 were settled before or during litigation by DoD and 1 by a private relief bill, 10 were terminated by denial, and the rest were still pending. As the report also noted, "Agencies have little or no incentive to settle a claim," and claimants, frustrated, often drop the matter. The House Committee on Government Operations, which prepared the report, found "little judicial guidance on First Amendment questions." It quoted an official of the Department of Justice on the question but was told that the Department "has thought it wise to follow a rule of self-restraint in expressing public views on constitutional questions presented by the statutes we are called upon to enforce."[62]

[60]"Brief U.S. Suppression of Proof Stirs Anger," *New York Times*, Feb. 17, 1987, p. C3.

[61]*The Government's Classification of Private Ideas*, Thirty-Fourth Report by the (House of Representatives) Committee on Government Operations, House Report No. 96-1540, 96th Cong., 2d sess., Dec. 22, 1980, p. 2.

[62]Ibid., p. 27.

This authority must be considered as part of the total burden on the exercise of free speech.

Imposition of a secrecy order can be avoided simply by not seeking a patent. (The information may nevertheless be subject to control as Restricted Data or under export controls.) Nevertheless, imposition of a secrecy order does operate as a restriction on traditional freedom of scientific communication. This authority must therefore be considered as part of the total burden on the exercise of free speech.

EXPORT CONTROLS

Export controls are also a form of legislated restraint on scientific communication. They are considered separately because national security is only one objective of these controls.

The Arms Control Act

This Act provides authority for restricting or prohibiting export of technical data related to defense articles.[63] It applies to blueprints, drawings, photographs, plans, instructions, software, and documentation. This Act is one of the U.S. Statutes used to restrict unclassified information.

Under the Arms Control Act, International Traffic in Arms Regulations (ITAR) are developed and a U.S. Munitions List is maintained by the Department of State, with the help of DoD. The regulations[64] operate in much the same way as regulations under the Export Administration Act, discussed below. ITAR, does not specifically exclude "fundamental research," but it does exempt general mathematical and engineering information that is only indirectly useful to military purposes. It is not clear whether any information exempted from Export regulations is restricted under ITAR.

The Export Administration Act

In 1976 a Defense Science Board panel headed by Fred Bucy reexamined the need for secrecy in scientific research, with special attention to the problem of "involuntary technology transfer" to hostile or competitive nations. The Bucy panel argued that the knowledge most vital to protect is not embedded in military weaponry per se, but knowledge that conveys design and manufacturing know-how. The export of technological information contained in scientific publications in some areas is harmful to the United States. These areas were "arrays of design and manufacturing know how," "keystone" manufacturing processes, inspection and test equipment, and products requiring sophisticated operation, application, and maintenance.

This recommendation was a significant expansion of the term "militarily useful." The transfer of design concepts and manufacturing processes can relate directly to the manufacture of weapons.[65] But a further, and ultimately more important point, may be the recognition that modern concepts of national security depend at least as much on the strength of the Nation's industrial base as on the stock of military weapons. There is a close tie between scientific information and industry strength and competitiveness.

[63]22 U.S.C. 2751.

[64]A revised version of ITAR became effective Jan. 6, 1985.

[65]A high government official noted to OTA, "The information used in manufacturing high-tech products used in weapons systems diffused into the civilian private sector and could no longer be controlled by DoD, at least to the extent that it once was. This recognition, above everything else, forced us to redefine what was militarily useful." (Private communication, June 19, 1987.)

There is a close tie between scientific information and industry strength and competitiveness.

The Bucy panel recommendations set in motion more vigorous efforts to control dissemination of technical knowledge related to militarily useful advanced technology, and led to the strengthening of export control laws in the following years.[66]

The Export Administration Act had already been passed in 1969, and was amended in 1979, 1981, and 1985. It controls the export of "goods and technology which would make a significant contribution to the military potential of countries which would prove detrimental to the national security. . . ."[67] Technology is defined to include "information and know how, whether in tangible form . . . or intangible form, that can be used to design, produce, manufacture, utilize, or reconstruct goods, including computer software and technical data . . ."[68] The Export Administration Act not only applies to information passing across our borders, but also limits access of foreign nationals to information in this country.

Regulations for administering and enforcing the Export Administration Act are promulgated by the Department of Commerce (DOC), and the products or areas covered are identified in a Commodity Control List, which is maintained by DOC with the help of DoD and DOE. The list specifies the countries to which each of about 100,000 items (in 1984) cannot be exported without a validated license. All export of unpublished technical data to Communist bloc countries requires a license. The United States is also a founding member of the multinational Coordinating Committee on Multilateral Export Controls (CoCom), which under multilateral agreements and procedures provides for cooperative control of exports to the Soviet bloc with restrictions on munitions, nuclear energy, and some other dual-use technologies. Many but not all of the items on the U.S. Commodity Control List are also on the International (CoCom) List.

The early use of export controls emphasized products more than information as such. Thus, when the Commerce Department halted shipment of magnetic computer tapes to Eastern bloc countries in 1982, "the action was taken to ban the medium, not the message."[69] Although these were standard IBM computer tapes, DOC said that Eastern European countries could not manufacture such high-quality tape and should not learn how from U.S. products.[70]

For U.S. exporters, restrictions on trade with the Eastern bloc nations may be less important than the effects of unilateral restrictions on trade with other Western nations. The Administration insists on such restrictions to curb the indirect flow of technology to the Soviet Union, because once information is outside the country it is outside of our control.[71] This imposes costs on U.S. exporters and causes friction with our trading partners. Some

[66]Stephen B. Gould, "Secrecy: Its Role in National Scientific and Technical Information Policy," *Library Trends*, summer 1986, p. 72. Gould was until mid-1987 Director of the Project on Scientific Communication and National Security, of the Committee on Scientific Freedom and Responsibility of the American Association for the Advancement of Science.

[67]50 U.S.C. 2402(2)(A) App.

[68]50 U.S.C. 2415 App.

[69]Roland W. Schmitt, "Export Controls: Balancing Technological Innovation and National Security," *Issues in Science and Technology*, vol. VI, fall 1984, p. 117. Schmitt is head of the General Electric Research and Development Center.

[70]Ibid. See also *Chemical & Engineering News*, "U.S. Bans Tape Exports to East Bloc," Sept. 20, 1982, p. 6. As a result, *Chemical Abstracts*, which had supplied its bibliographic tapes to Warsaw Technical University since 1974, did not get its export license renewed. The Institute for Scientific Information, a commercial firm providing bibliographic services, could no longer send its standard tapes to customers in Poland, the U.S.S.R., and Hungary, but could send the same information on low-quality tapes.

[71]Export Administration Regulations require prior authorization from the Office of Export Licensing in certain situations before foreign products that incorporate parts, components, or materials of U.S. origin, can be exported from one foreign country to another. Until recently, all foreign companies needed permission from DOC before reexporting a product that contains any U.S. components, even a microchip. New regulations effective in 1987 somewhat simplified the procedure for requesting such authorization and exempted foreign-manufacturer products destined for some countries when the U.S. content is no more than 20 percent by value. (15 CFR Parts 376 and 385; *Federal Register* 51, No. 129, July 7, 1986, 24533.)

foreign companies have notified their U.S. suppliers that they are "designing out" U.S. parts to avoid this additional effort; others consider this additional cost in deciding on suppliers.[72] Many U.S. industry leaders have protested export controls.[73]

Export controls apply not only to commercial products but to technical data, research reports, and some other kinds of information as well. A Defense Science Board Task Force on University Responsiveness to National Security Requirements, in early 1982, found that the shift in emphasis in export controls from products to technological information was seriously disturbing the relationship between the government and universities.[74] The Task Force recommended that "clearer guidelines," not overly restrictive, be formulated for DoD-funded university research with the help of universities. This recommendation however led to new confusion and dispute over the basis for applying either classification or export controls. In theory, they involve quite different objectives, standards, and procedures, but in practice they are often seen as alternatives.

When the 1979 Export Administration Act was about to expire in 1983, efforts to rewrite the bill revealed sharply divergent concerns. Some in Congress sought to strengthen export controls, while others argued that excessive controls reduced the competitiveness of U.S. companies and contributed to our trade deficit.[75] There were hearings in both the Senate and House. The House accepted a provision proposed by the Committee on Foreign Affairs, which read:

> It is the policy of the U.S. to sustain vigorous scientific enterprise. To do so requires protecting the ability of scientists and other scholars freely to communicate their research findings in accordance with applicable provisions of the law, by means of publication, teaching, conferences, and other forms of scholarly exchange.[76]

Although the House wished to avoid "overly broad interpretation" of the Export Administration Act, the Senate Committee on Banking added a provision making academic institutions subject to requirements of the commercial agreements provision. This meant that university agreements with certain foreign countries must be reported to the Department of Commerce. Some believe that this gives government a "ready opportunity to regulate, through the application of export controls, the content of lectures, conference presentations, teaching, and publications by U.S. academics in certain foreign countries."[77] Others insist that there is no necessary connection between "recording commercial transactions after the fact," and "controlling scientific information before the fact."

The House and Senate failed to agree on reauthorization of the Act in conference. The President then issued Executive Order 12470 (Nov. 14, 1983), declaring a national emergency and activating the same powers under the International Emergency Powers Act.

The Export Administration Act was finally reauthorized in April 1985. The new law attempted to streamline its procedures but did not reduce the number of items covered. GAO has said that "The government continues to require export licenses for more dual-use items than is necessary to protect national security."[78] Dual-use items are devices, systems, or "know-how" that have both military and nonmilitary applications.

Revisions to the implementing regulations under the Act in 1986 exempted "fundamen-

[72]Don Bonker, "Protecting Economic Interests," *Issues in Science and Technology*, fall 1986, p. 100.

[73]According to officials in the Department of Commerce Export Administration Program Review Staff, "The possibility of reverse engineering [indirect leakage of useful information as a result of West-West trade] has been discounted by many exporters who claim that their manufacturing techniques cannot be derived by examining the finished products." (Direct communication to OTA project staff, June 19, 1987.)

[74]U.S. Department of Defense, *Report of the Defense Science Board Task Force on University Responsiveness to National Security Requirements* (Washington, DC, 1982).

[75]Don Bonker, "Protecting Economic Interests," *Issues in Science and Technology*, fall 1986, p. 100.

[76]50 U.S.C. 2402 (12) App.

[77]Harold C. Relyea, *National Security Controls and Scientific Information*, Congressional Research Service Issue Brief B82083, updated June 17, 1986, pp. 12-13.

[78]U.S. Congress, General Accounting Office, *Export Control Regulation Could Be Reduced Without Affecting National Security*, May 26, 1982.

In January 1987 the National Academy of Sciences and the National Academy of Engineering issued a report sharply critical of the implementation of export controls.

tal research" from export controls, using the definition of fundamental research introduced in NSDD 189, September 1985, which is discussed below.[79] University research is normally considered "fundamental" unless scientists have accepted prior restrictions on publications through contract agreements.[80]

The DoD Appropriations Act for fiscal year 1984 gave the Secretary of Defense authority to withhold from public disclosure, under the Freedom of Information Act (FOIA), any technical data with military or space application already under control of DoD, if that data would fall under Export Acts. DOE policy is to use this authority only if the data has "military centrality," and requires the recipient to promise not to reveal the information to the public. This avoids releasing the data from effective government controls.[81]

In January 1987 the National Academy of Sciences and the National Academy of Engineering issued a report sharply critical of the implementation of export controls. It said that the Administration had "tended to focus on tightening controls while giving little attention to their effectiveness and cost"; by trying to impose its own export restrictions on countries that import U.S. technology, the Administration had injured both U.S. competitiveness and relations with our allies. The Department of Defense has been given too large a role in export policy, the panel implied, being more concerned with national security than with the competitive strength of American industry.[82]

The Export Administration Act has a legitimate government purpose other than restricting speech.

Many question the effectiveness of export controls. One expert has been quoted as saying that "the avenues for transfer open to Russia are so broad that they are almost impossible to control," adding that the primary avenue is probably through Western plant workers and junior executives recruited over the past 30 years in the United States and Western Europe.[83]

The Constitutionality of Export Controls

It is assumed that any impingement on First Amendment rights under the Arms Export Control and Export Administration Acts is incidental, because these regulations have a legitimate government purpose other than to restrict speech and press.[84] The Court might

[79]15 CFR 379, May 16, 1986. The regulations say that information resulting from fundamental research qualifies for unrestricted export to any destination under a General License GTDA, that is, a "general license for technical data available to all destinations."

[80]Unclassified contract research funded by DoD under budget category 6.1 is considered fundamental research, and most unclassified research at universities funded under budget category 6.2 is also considered fundamental research. Contract research done in off-campus university facilities and not supported under budget category 6.1 is however generally not automatically considered fundamental research, but may still be free of restrictions. Research done by business or industry is considered fundamental research only if the researchers are free to make it available without pay or restrictions (i.e., it is not proprietary) and it is not classified.

[81]Communication to OTA from officials in the Office of the Secretary of Defense, May 1987.

[82]National Academy of Science, Panel on the Impact of National Security Controls on International Technology Transfer, *Balancing the National Interest: U.S. National Security Export Controls and Global Economic Competition*, Washington, DC, 1987. The report was prepared by a panel chaired by Lew Allen, Director of the Jet Propulsion Laboratory. The panel recommended that the United States rely on, and seek to improve, the Multilateral Export Controls Coordinating Committee (CoCom) consisting of the NATO countries plus Japan and France.

[83]Frederick Kempe, "Losing Battle: Keeping Technology Out of Soviet Hands Seems To Be Impossible," *Wall Street Journal*, July 24, 1984, p. 1.

[84]*Adderly v. Florida*, 385 U.S. 39 (1966); *Brown v. Louisiana*, 383 U.S. 131 (1966); *Kovacks v. Cooper*, 336 U.S. 77 (1949); *Breard v. Alexandria*, 341 U.S. 622 (1951); *O'Brien v. United States*, 391 U.S. 367 (1968).

tend to give them the benefit of the doubt, as in the only case[85] so far that directly challenged the applicability of the Arms Export Control Act to unclassified data. This case involved business rather than scientific interests. Edler provided technical assistance to French companies on tape-wrapping techniques that had both commercial and military applications, despite rejection of Edler's application for an export license. The U.S. Court of Appeals said that Edler had some First Amendment rights with respect to the transaction, but concluded that the Arms Export Control Act was a "general regulatory statute, not intended to control the content of speech but incidentally limiting its unfettered exercise,"[86] and might, therefore, be constitutionally permissible.

Observing that a broad interpretation of "technical data" would "seriously impede scientific research and publishing and the international scientific exchange," the court adopted a narrow construction that limited technical data to that which "relates in a significant fashion to some item on the Munitions List," as opposed to being "merely vaguely useful for the manufacture of arms." Moreover, it is necessary that the relationship to that item be clear and that the defendant know or have reason to know that the data was intended for a prohibited use.[87]

The court's explicit sensitivity to the necessity for protecting open dissemination of scientific knowledge offers hope that the statute cannot be applied in a manner that interferes with traditional modes of scientific communication. The Office of Legal Counsel of the Department of Justice addressed this issue in separate communications to the Secretaries of Defense and Commerce in July 1981, asserting that export control regulations may not impinge on scientific communication unless the "speech" is directly related to a business transaction.[88] Nevertheless, some critics maintain that this distinction has not been adhered to in the ensuing 6 years.

[85]*United States* v. *Edler Industries, Inc.*, 579 F.2nd 516 (9th Cir., 1978).

[86]Ibid. at 520, citing *Konigsberg v. State Bar*, 366 U.S. 36, 50-55 (1961).

[87]Ibid., pp. 520 and 521

[88]Harold C. Relyea (ed.), "Shrouding the Endless Frontier—Scientific Communication and National Security: The Search for Balance," *Striking a Balance: National Security and Scientific Freedom* (Washington, DC: American Association for the Advancement of Science, 1985), p. 90-92.

Chapter 5

The 1980s: Converging Restrictions on Scientific Communications

CONTRACTUAL RESTRICTIONS ON COMMUNICATIONS

Most universities are reluctant to undertake classified research, but many are willing to accept contractual restrictions that have the same effects.

Dissemination of scientific information or technical data[1] can be and often is restricted by the terms of written agreements between government funding agencies and nongovernment researchers. Most universities are reluctant to undertake classified research, but many are willing to accept contractual restrictions that have the same effects. In some cases, indeed, refusal to accept such contracts is considered by faculty to be an infringement on their academic freedom. Some civil libertarians, on the other hand, object to such contracts. While a contract, freely entered into, is assumed to benefit both parties to it, this does not provide for consideration of the public interest (and investment) in scientific knowledge, which may not entirely coincide with or be limited to national security interests.

The government often requires that contractors and grantees agree to submit publications resulting from nonclassified government-sponsored research for prepublication review. This raises the question of prior restraint. There are, however, no reported court decisions involving prepublication review clauses in contracts and grants to universities.

National Security Decision Directive 84 (NSDD 84),[2] issued on March 11, 1983, requires all present and future government employees to sign a lifetime nondisclosure agreement as a condition for access to classified information, or to "Sensitive Compartmented Information" (SCI). Federal classifying agencies have the right of pre-review of public statements, lectures, and speeches. Contacts between media representatives and agency personnel are controlled. This directive was aimed primarily at Federal employees, but secrecy agreements can also be required of government contract researchers under the directive.[3]

According to a recent study supported by the Fund for Investigative Journalism, by the end of 1985 more than 290,000 individuals had signed lifetime prepublication review agreements (Non-disclosure Agreements Standard Forms 189 and 189A) under NSDD 84, and more than 14,000 speeches and articles had been submitted for review.[4] There have been strong protests against the requirement for lifetime agreements. However, the Federal Government takes the position that the contractual obligation of an employee overrides First Amendment protections.

In *Snepp* v. *United States*[5] the Supreme Court found no constitutional impediment to enforcing such an agreement. This case, however, involved CIA employees, and the intelli-

[1] As already noted, national security officials tend to make a sharp distinction between "scientific" communications and technical/technological exchanges that is not always either clear or acceptable to researchers in an area.

[2] The nature of National Security Decision Directives is discussed below.

[3] Secrecy agreements or contracts used within the intelligence community were found to be a proper enforcement device in 1980 by the Supreme Court (*Snepp* v. *U.S.*, 444 U.S. 54).

[4] Donna DeMoc, "Sworn to Silence," *The Progressive*, May 1987, p. 29. The study presumably covered SF 189s; SF 189A was approved for inclusion in the Industrial Security Manual in late April 1987.

[5] 444 U.S. 507 (1980).

gence community is generally conceded to have particularly strong interests in internal security. Two Circuit Court decisions, one before and one after *Snepp*,[6] indicate that such an agreement might not be enforceable if classified information is not involved. These cases did not involve research results or scientific information.

NSDD 84 also sought to expand the use of "lie detectors" by Federal agencies. Executive branch employees can be required to submit to polygraph examinations for access to certain classified information, or in the course of investigations of unauthorized disclosure of classified materials. The threatened expansion of polygraph use brought strong protests. In the fall of 1983, Congress temporarily prohibited implementation of the polygraph provision, and President Reagan agreed not to pursue this policy immediately.[7] In effect, the provisions of NSDD 84 dealing with polygraphs have been rescinded, except as they pertain to DoD, where polygraph tests are widely used not only in investigations but for routine screening of recruits, promotions, etc.

[6]The first was *United States* v. *Marchetti*, 366 F.2d 1309 (4th Cir., 1972). *cert. den.*, 409 U.S. 1063 (1972). The second was *McGehee* v. *Casey*, 718 F.2d 1137 (D.C. Cir., 1983).

[7]Harold C. Relyea, *National Security Controls and Scientific Information*, Congressional Research Service Issue Brief B82083, updated June 17, 1986, p. 69. See also National Academy of Sciences, Committee on Science, Engineering, and Public Policy, Panel on Scientific Communication and National Security, *Scientific Communication and National Security*, 1982.

RESTRICTIONS ON INFORMAL COMMUNICATIONS

Classification, legislative mandates, contract agreements, and export controls have all been used in the last decade to restrict *informal* communications among scientists.

Classification, legislative mandates, contract agreements, and export controls have all been used in the last decade to restrict informal communications among scientists. By informal communications is meant modes of communication other than formal publishing: speaking, classroom teaching, participation in professional meetings and seminars, and similar activities. Restrictions on campus teaching are particularly irksome to many scientists. Since the 1970s, there has been a steady influx of foreign students to U.S. universities. Any restrictions on who may be taught what in a university are of profound importance, infringing on academic freedom, on institutional responsibility, and on the prestige and economic viability of the institution.

In 1980, the Department of State informed Cornell University that a visiting Hungarian engineer would have to be limited to classroom pursuits and could not participate in certain professional seminars or receive prepublication copies of research papers. Rather than abide by these restrictions, the university canceled his visit. Later that year, the Department of State, acting under export restrictions, asked universities to prohibit visiting Chinese students from engaging in certain studies.[8] There were reports of a few instances in which universities, in ill-considered, hasty responses, listed short courses or seminars "for U.S. citizens only;" such decisions were apparently few, and were soon terminated.[9]

On February 27, 1981, the presidents of five leading universities (Stanford, the California Institute of Technology,the Massachusetts Institute of Technology, Cornell, and the Univer-

[8]Relyea, op. cit., p. 4.

[9]There were references in the press at that time to university courses or seminars so advertised, but recent discussions with a number of education association officials identified only one specific incident of a course listed "for U.S. citizens" at a university, and that decision was said to have been quickly overruled.

Scientific exchange is a primary purpose and role of professional societies.

sity of California) sent a letter of protest to the Secretaries of Commerce, State, and Defense. The university presidents said that the government had resorted to measures that could "irreparably harm university-based research."[10]

Scientific exchange is a primary purpose and role of professional societies. These organizations depend on their members to judge whether communication of research results or other information violates national security restrictions, and they can be faced with dilemmas when their members either intentionally or inadvertently transgress. In February 1980 there were strong efforts by the Carter Administration to regulate the communication of scientific information by professional societies. When the American Vacuum Society organized an international meeting on magnetic bubble memory devices, the Department of Commerce notified the society that the expected presence of nationals of certain foreign countries subjected the proceedings to compliance with export licensing. The Association promptly rescinded invitations to scientists from Hungary, Poland, and the U.S.S.R. Chinese scientists, already en route, were allowed to attend after signing an agreement not to "re-export" to nationals from 19 countries what they learned.[11]

In August 1982, 4 days before a meeting of the Society of Photo-Optical Instrumentation Engineers (SPIE), DoD learned that four Soviet scientists were to attend. DoD confiscated a dozen papers from DoD employees who were to present them at the meeting, and notified

[10]Gina Bara Kolata, "Attempts To Safeguard Technology Draw Fire," *Science*, vol. 212, No. 4494, May 1981, p. 523. The letter also said: "There is no easy separation in any engineering curriculum. . . . Furthermore, producing graduates with no 'hands on' experience in these areas would be of little value to American high technology industries."

[11]Ibid., p. 3.

Under current DoD directives, unclassified papers containing export-controlled information cannot be presented at professional and academic meetings unless dissemination and access controls are "equivalent to those used for distributing the data directly by DoD."

the organizers that other papers were sensitive. DoD representatives were present as the meeting began and questioned participants as to whether their papers resulted from work sponsored by DoD and whether they had received clearance. One hundred papers were withdrawn. A SPIE official later said that government officials had overreacted to the presence of Soviet citizens, and that SPIE members themselves had probably panicked at the sudden crackdown. Many of the papers that had been hurriedly withdrawn were later cleared and published or presented, although others were found to deal with classified research.[12]

Under current DoD directives, unclassified papers containing export-controlled information cannot be presented at professional and academic meetings unless dissemination and access controls are "equivalent to those used for distributing the data directly by DoD"[13]—so-called unclassified/limited access presentations.[14] This rule was applied on an ad hoc basis during another meeting of the Society for Photo-Optical Instrumentation Engineers in April 1985. Two weeks before the meeting, organizers were notified by DoD that a special session, organized by one of its members at a military base, with 43 papers scheduled,

[12]This account is based on discussion with SPIE director Joseph Yaver in May 1987; for a contemporary account, see Joel Greenberg, "Science's New Cold War," *Science News*, vol. 123, Apr. 2, 1983, p. 218. Also see Relyea, op. cit., 1986.

[13]Statement supplied for OTA by DoD officials, Office of the Secretary of Defense.

[14]U.S. Department of Defense, Office of the Under Secretary of Defense for Research and Engineering, "Policy and Guidelines for the Presentation of DoD Sponsored Scientific and Technical Papers," draft proposal, Oct. 24, 1985.

would have to be canceled because the papers could not be given in open sessions. The meeting organizers and an official from the DoD Office of Research and Advanced Technology worked out a compromise designed to salvage as many presentations as possible. After hectic review and revisions, 28 of the papers were presented in "closed" sessions, at which attendees were screened and required to sign the agreement used to control distribution of export-controlled DoD technical data.[15]

SPIE officials emphasize that the compromise was worked out in a friendly spirit and in good faith by both sides, but the society insists that the compromise was a "one-time necessity" and not a precedent. SPIE now dissociates itself from classified, controlled-access meetings or sessions that may be arranged by its members, but acknowledges that such meetings are held in parallel or immediately following society meetings and are regarded by many members as desirable and necessary.

Other professional societies admit uncomfortably to similar situations. They officially oppose and disclaim closed or limited access sessions that do not serve all members (especially when only non-U.S. citizens are excluded, since most identify themselves as international societies); yet recognize that such meetings are organized by members in parallel with society meetings—"a bit of a fiddle," one society official says. In 1984 the American Association for the Advancement of Science compiled a list of 12 events in which professional societies limited their traditional information dissemination function or activities to comply with security policies. For example, one session at a professional association meeting required participants to bring to the session proof of citizenship.[16] However, on September 17, 1985, a Joint Communication was sent to the Secretary of Defense from the elected presidents of 12 scientific and engineering societies, protesting DoD actions. It stressed the value to the Nation of open exchange of scientific information, pointing out that such exchange is necessary to validate findings, to cross-fertilize scientific knowledge and activity, and to avoid duplication of effort. The society presidents argued that secrecy hurts the national position in science, technology, and industrial competitiveness more than it strengthens national security. They notified the Secretary of Defense that they will not "be responsible for, nor will sponsor, closed or restricted-access sessions" in the future.[17]

DoD again, in April 1986, issued clarification of its procedures in screening papers on unclassified DoD-sponsored research for presentation at meetings. DoD says it will review papers under specific time frames (10 to 30 days) to help avoid last minute pressure for withdrawals. However, the statement also made clear that information deemed classified could be presented only on DoD premises, and unclassified information would still be subject to export control laws. Furthermore, the sponsors of scientific meetings are responsible for limiting access to authorized individuals (which societies say they cannot do).[18] Some DoD officials, and some "neutral observers," say that these actions have effectively alleviated professional concerns; a number of professional society officials consulted by OTA report that this issue remains one of active and strong concern to their societies and to most of their members. A nongovernmental science policy specialist asserts that DoD, in practice, has been far less strict and less restrictive than their official policy guidelines and directives indicate they will be or should be. On the other hand, a scientist and society administrator argues forcefully that DoD policies have an "extraordinarily chilling effect" on scientific communication because scientists, fearful of prejudicing the essential source of funding for future research, lean over backwards and probably restrict themselves more than is absolutely required.

[15]This account was developed from discussions with both SPIE and DoD officials in May 1987 and differs in some details from accounts in the general and specialist media at the time (1985) and soon thereafter.

[16]Relyea, op. cit., 1986.

[17]American Association of Engineering Societies, *Policy and Engineering Priorities, 1986*, Washington, DC, 1986.

[18]Ibid.

The constitutional issue has not often been explicitly raised, possibly because Congress has appeared to add its authority to that of the executive agencies.

The export control statutes appear to provide a legal basis for restricting economic activities and scientific communication—formal and informal—within the United States as well as across its borders, since publication in U.S. journals is tantamount to worldwide publication. As already discussed, however, their constitutionality has not really been tested. The constitutional issue has not often been explicitly raised, possibly because Congress has appeared to add its authority to that of the executive agencies. Scientists instead have tended to try to minimize the opportunity for government intervention through a strategy of "self-restraint."

SELF-RESTRAINT

The strategy of self-censorship could be a significant limitation on dissemination of scientific thought and on the exercise of constitutional freedoms.

The strategy of self-censorship poses an interesting ethical question. The objectives in self-censorship may be the exercise of reason, self-control, and patriotism, and the desire to avoid provoking authoritarian restrictions; but the end result could nevertheless be significant limitation on dissemination of scientific thought and on the exercise of constitutional freedoms.

In 1982, at the annual meeting of the American Association for the Advancement of Science (AAAS), CIA Deputy Director Admiral Bobby Inman said in a public address:

> A potential balance between national security and science may lie in an arrangement to include in the peer review process (prior to the start of research and prior to publication) the question of potential harm to the nation.[19]

Earlier, as Director of the National Security Agency (NSA), Inman had tried to take control over government-funded cryptography research from the National Science Foundation (NSF).[20] Having failed, he urged the American Council on Education to form a public cryptography study committee, which then recommended a voluntary system for prepublication review by NSA of manuscripts on cryptography. In 1981, NSF adopted a policy of requiring such prepublication review on "potentially classifiable results" coming from its research grants.

In his AAAS speech, Inman included not only cryptography but other areas in his argument for self-monitoring or self-censorship: computer hardware and software, electronic gear and techniques, lasers, crop projections, and manufacturing processes. He warned bluntly that if this was not done voluntarily, "public outrage" would produce laws further restricting publication of scientific work that government considered sensitive. Inman repeated this warning 3 months later at a congressional hearing held by two subcommittees of the House Science and Technology committee,[21] and said

[19]Relyea, op. cit., June 1986, p. 2.

[20]Competing scientific, industry, and national security interests in the development of encryption and related techniques and technologies for safeguarding data in computer and telecommunications systems has made this scientific technology particularly troubled by the tensions between national security restrictions and other societal priorities, as described in this chapter.

[21]U.S. Congress, House of Representatives, Committee on Science and Technology, Subcommittees on Science, Research, and Technology, and Investigation and Oversight, *Impact of National Security Considerations on Science and Technology Hearings*, 97th Cong., 2d sess., Mar. 29, 1982.

that unless Soviet access to American science, technology, and industrial information was voluntarily controlled, there would be a move by the government to further regulation.

Inman directly recognized that:

> . . . Science and national security have a symbiotic relationship. . . . In the long history of that relationship, the suggestion is hollow that science might (or should somehow) be kept apart from national security concerns, or that national security concerns should not have an impact on "scientific freedom."[22]

[22]Inman, a statement in *Aviation Week & Space Technology*, "Classifying Science: A Government Proposal . . . And a Scientist's Objection," Feb. 8, 1982, p. 10.

Protests were immediately raised about Admiral Inman's new call for self-restraint. The Executive Director of AAAS said:

> He has asked that research scientists submit voluntarily to open-ended censorship by the CIA or face the likelihood of being forced to do so by Congress. Even in wartime, such a demand would be an extreme one, and in the absence of national security emergency it is incongruous. It raises troubling questions involving both scientific freedom and the force of constitutional provisions against arbitrary government.[23]

[23]Ibid., statement by William Carey, Executive Officer, AAAS.

NATIONAL SECURITY DIRECTIVES AND THE ROLE OF THE NATIONAL SECURITY AGENCY

National Security Directives

NSDD 84, in 1983 (discussed above), marked the first general public knowledge of National Security Decision Directives (NSDD) as a form of Presidential directive distinct from Executive Orders and Proclamations.[24] Executive Orders and Proclamations are always published. About 200 NSDDs have been issued by President Reagan since 1981, but only 5 have been publicly disclosed, the rest being classified. Between 1947 and 1981, other presidents had issued "National Security Action Memorandums" and "Presidential Directives" which like NSDDs were kept secret, from both the public and from Congress. They are all thought to be associated with the National Security Council, created within the Office of the President in 1947.

NSDD 189

In late 1982, after the recommendations of the Corson panel, President Reagan had ordered his Office of Science and Technology Policy (OSTP) to coordinate an interagency review

[24]Harold C. Relyea, Congressional Research Service specialist in American National Government, testifying before the House Committee on Government Operations on H.R. 145, Mar. 17, 1987. CRS press release.

"It is the policy of this Administration that, to the maximum extent possible, the products of fundamental research remain unrestricted."

of the issue of government secrecy (National Security Study Directive 14-82). The review was itself classified, so that there was no input from universities or other nongovernment sources. OSTP's report was due on March 1, 1983, but did not appear. There were rumors and stories in science policy newsletters that the Administration was about to announce new formal controls over "sensitive fundamental research," i.e., a fourth category of classification below that of "confidential." But such a strategy would involve both monetary and political costs. Classified information requires special procedures, controlled facilities, etc. Contractual agreements between researchers and funders are less expensive, legally defensible, and less likely to evoke protests.[25]

[25]DoD was in fact considering a fourth security classification at this time, according to sources in the Pentagon, to protect "military operational data and high tech data—not fundamental research." (Communication to OTA May 1987.)

Instead of the long-delayed report from OSTP, in May 1984, DoD's Deputy Under Secretary for Research and Advanced Technology, Dr. Edith Martin, unexpectedly released a draft Decision Directive that was to become NSDD 189. Signed on September 21, 1985, NSDD 189 said:

> It is the policy of this Administration that, to the maximum extent possible, the products of fundamental research remain unrestricted. . . . Where the national security requires control, the mechanism for control of information generated from federally-funded fundamental research . . . at colleges, universities, and laboratories is classification . . . . No restrictions may be placed on conduct or reporting of [such] research that has not received national security classification, except as provided in applicable U.S. Statutes.

It was not clear what was encompassed in the term "fundamental research," a term not until then in common use. Since the "applicable U.S. Statutes" include the Export Administration and Arms Export Control Acts, critics said that this directive did not materially change the existing situation, except that either more Federal agencies would have power to classify, or DoD's scope of authority would broaden. More scientists would become subject to NSDD 84 and be required to sign lifetime nondisclosure contracts. National security officials on the other hand deny this because "fundamental research" is excluded from export controls and there is no evidence that DoD is overusing classification procedures.

NSDD 189 was interpreted by some as an effort to "cool the campus secrecy issue" by dropping the idea of further controls in "gray areas" (between classified and unclassified research).[26] But in a memo accompanying NSDD, the White House stressed that it "preserves the ability of the agencies to control unclassified information using legislated authority provided expressly for that purpose in applicable U.S. statutes."

A memorandum written by Under Secretary of Defense Richard DeLauer on October 1, 1984, to reassure the universities, again specified that no restriction would be put on publication of fundamental research sponsored by DoD. It defined fundamental research to include virtually all of that done on university campuses, with rare exceptions "where there is a likelihood of disclosing performance characteristics of military systems, or of manufacturing technologies unique and critical to defense." In these cases, restrictions must be put into the research contract.

The Role of the National Security Agency

The Brooks Act of 1965 gave the National Bureau of Standards authority for developing technical standards for computer systems. Private firms were developing an interest in this market, and commercial security devices meeting NBS standards were developed for computers. During the mid-1970s, a government-certified cryptographic algorithm and a "public-key" algorithm were announced (in the open literature), and inexpensive security devices were developed commercially.

Presidential Directive/National Security Council 24 (PD/NSC-24), issued by President Carter in 1977, said that nongovernmental telecommunications information "that would be useful to an adversary" would be identified, and the private sector informed of the problem and encouraged to take appropriate actions.[27] This was a clear sign that the Federal Government, DoD in particular, would take a stronger hand in telecommunications security.

The Secretary of Defense was to be responsible for protecting government communications, both classified and now "unclassified but sensitive" communications. The Secretary of Commerce would be responsible (through NTIA) for government-derived unclassified data not related to national security, and would

[26] *Science and Government Report,* "White House Decides To Cool Campus Secrecy Issue," vol. XIV, No. 11, June 15, 1984; Colin Norman, "Universities Prevail on Secrecy," *Science,* vol. 226, No. 26, October, 1984, p. 418.

[27] National Telecommunications Protection Policy (unclassified), Feb. 9, 1979, unclassified excerpts from Presidential Directive/NSC-24, Nov. 16, 1977, classified.

NSDD 145 worried civil libertarians because of the broad scope of nonclassified information to be protected and because of the central role given to NSA, an agency outside of the usual modes of accountability.

deal with the private sector to "enhance their communications protection and privacy." The Defense and Commerce Departments attempted to develop a joint proposal for a national policy on cryptography but were unable to reach agreement, They submitted separate proposals which, however, were never acted on by the President's Science Advisor.[28]

NSDD 145 and HR 145

National Security Decision Directive 145 (NSDD 145), September 17, 1984, superceded PD/NSC-24, and made NSA the central agency ("Executive Agent") for development and choice of cryptography-based technology for the security of unclassified, but sensitive information in telecommunications and computer systems of all government agencies.* This seems to apply whether the information concerns national security or not, and regardless of whether the technology is to be used for security or for authenticating transactions.

In short, NSDD 145:

- broadened NSA protection to encompass unclassified information in telecommunications and automated information systems;
- assigned to NSA the full responsibility for developing and advising of safeguard technology and for making decisions about technical standards, ignoring the role of NBS under the Brooks Act; and
- established an interagency group to implement and enforce NSDD 145 policy.

This announcement worried civil libertarians because of the broad scope of nonclassified information to be protected and because of the central role given to NSA, an agency outside of the usual modes of accountability. From the time it was issued, there have been conflicting interpretations and official pronouncements about the details of what it means. At first, "sensitive information" was defined as "unclassified but sensitive national-security-related information." In June 1985, Donald Latham, Assistant Secretary of Defense and Chairman of the National Telecommunications and Information Systems Security Committee (NTISSC) established under NSDD 145, said that "sensitive" information might include anything from crop forecasts to personnel records.[29] Three months later, in testifying before the Committee on Government Operations, September 18, 1985, Mr. Latham said specifically that "non-national-security-related" information was not included in the purview of NTISSC. But in October 1986, an NSA memoradum, NTISSP No. 2,[30] extended this purview to:

> Other government interests . . . related but not limited to the wide range of government or government-derived economic, human, financial, industrial, agricultural, technological, and law enforcement information, as well as the privacy or confidentiality of personal or commercial proprietary information provided to the U.S. government by its citizens (Section II, Definitions).

The NSA policy announcement also said:

> The NSDD-145 Systems Security Steering Group has established that sensitive, but un-

[28]For a more detailed treatment of the Government's role in computer and communications security, see U.S. Congress, Office of Technology Assessment, *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information*, OTA-CIT-310 (Washington, DC: U.S. Government Printing Office, October 1987).

*The National Security Agency was established by Executive Order in 1952, during the "Cold War," to carry out "signals intelligence" against hostile countries (i.e., to intercept and decode information they were sending through electronic communications) and to safeguard U.S. classified information against similar actions by those countries.

[29]U.S. House of Representatives, Committee on Science and Technology, Subcommittee on Transportation, Aviation, and Materials, *Hearings on Computer Security Policies*, June 27, 1985, statement of Donald Latham.

[30]National Policy on Protection of Sensitive but Unclassified Information in Federal Government Telecommunications and Automated Information Systems, NTISSP No. 2, Oct. 29, 1986.

> classified information that could adversely affect national security or other Federal Government interests shall have system protection and safeguards; however the determination of what is sensitive but unclassified information is a responsibility of Agency heads.

It now appears that the definition of "sensitive" could be applied to almost any information, or at least a very broad range of information, even if it is already published or available. NSDD 145 applies not only to Federal agencies but also to their contractors who electronically transfer, store, process, or communicate sensitive but unclassified information. It gives NSA the dominant role in developing the technology to be used, or deciding which technology will be used, by private sector organizations affected by the directives. NSA and DoD, however, emphasize that "protection" in this context literally means guarding against unauthorized access and malicious misuse by "hackers."

This new role for NSA would have gone beyond *development of technology* to involvement in decisions about the *content* of information, in order to prescribe what kind of security is appropriate. In late 1985 there had been signs of renewed government concern about the "leakage" of information from campuses and through commercial databases. The Pentagon released a CIA report, *Soviet Acquisition of Militarily Significant Western Technology: An Update*, based on Soviet documents. It listed 62 American universities "targeted for scientific and technical espionage" aimed at information about applied technology and engineering but also including "fundamental research for both Soviet military- and civilian-related science developments." This scientific and technological data is often in commercial electronic databases providing services to business and the public:

> The individual abstracts or references in government and commercial data bases are unclassified, but some of the information, taken in the aggregate, may reveal sensitive information concerning U.S. strategic capabilities and vulnerabilities. . . .[31]

[31] *Science and Government Report*, Oct. 1, 1985. The report released by Secretary of Defense Weinberger was an "update" of a declassified Central Intelligence Committee report originally released in 1982 by the Senate permanent subcommittee on Investigations. Dan Morgan, "Stolen U.S. Technology Boosts Soviet Strength, Report Says," *Washington Post*, Nov. 15, 1982.

There is a strong concern that DoD may require private sector database operators, at a minimum, to provide the government with lists of their subscribers, to place limits on foreign subscribers, and to increase the use of password protection and encryption.

The report went on to say that "One solution apears to be to thoroughly screen all candidate database entries and keep sensitive government information out of the public databases . . ." but added, "Unfortunately, this may also inhibit the United States' own national research effort by resisting the ready availability of such information."

It was clear that NSDD 145 had already given NSA the decisive role in prescribing security measures for government's automated databases, as well as telecommunition systems, but its authority over commercial databases is still in dispute. Diane Fontaine, director of information systems in the office of the Assistant Secretary of Defense, reportedly said at a meeting of the Information Industry Association, November 11, 1986: "The question is not should there be limits [on information in commercial databases] but instead what those limits should be."[32] Ms. Fontaine has since stated that she was misquoted and was referring only to government databases, but many auditors understood the reference as being to commercial databases. There is a strong concern that DoD may require private sector database operators, at a minimum, to provide the government with lists of their subscribers, to place limits on foreign subscribers, and to in-

[32] Quoted by Johanna Ambrosio, "Attempts To Restrict Private Data Bases Vex Industry," *Government Computer News*, Dec. 15, 1986. Another reporter's version was "The question is not whether we are going to protect information; the question is where the controls will be applied." Irwin Goodwin, "Making Waves: Poindexter Sails Into Scientific Data Bases, *Physics Today*, January 1987, p. 52.

crease the use of password protection and encryption.

In 1986 there were 3,200 electronic databases available worldwide through 486 online information services; 70 percent of these databases are produced in the United States, and all but two of the 20 largest database companies are American corporations.[33] Throughout much of 1986, a U.S. Air Force team visited commercial database owners to inquire about the extent of foreign access to these databases.[34]

Nonclassified government databases, even those specifically set up to provide better public access to information that is in the public domain, are in some cases already restricting access. An internal NASA memo of September 29, 1986, labeled "The So-called 'No-No' list,"[35] provides names of 33 organizations or individuals who are not to be "provided with subscriptions to NASA Tech Briefs, technical support packages, or other Technology Utilization documentation." The memo adds that "all embassies and consulates in the U.S. and representatives of foreign companies or organizations are to be included in this list." NASA Technology Utilization is a service to disseminate technical information to the public. Its information is not classified.

As major opposition to the thrust of NSDD 145 developed within Congress, a new National Security Advisor, Frank Carlucci, who had succeeded Mr. Poindexter, decided to review NSDD 145. His "key objective [was] finding a mechanism to eliminate any possible ambiguity regarding the role of the National Security Advisor in connection with the Systems Security Steering Group," and Carlucci instructed his staff "to initiate the procedures and prepare the papers necessary to rescind" NTISSP 2.[36]

H.R. 145

NSA had expanded its role into areas legislatively assigned to the National Bureau of Standards (NBS). H.R. 145, the Computer Security Act of 1987, was accordingly introduced. It would assign to NBS the responsibility for developing and promulgating standards and guidelines for safeguarding unclassified sensitive information in Federal systems, and for helping both civilian agencies and the private sector in using computer security safeguards.[37] This bill was passed by the House in July 1987, but had not been taken up by the Senate as of early January 1988.

---

[33]Information supplied by Information Industry Association. See *Potential Government Restrictions on United States Unclassified Commercial Databases*, Mar. 9, 1987, available from the association.

[34]Ibid., see also: Michael Schrage, "U.S. Seeking To Limit Access of Soviets to Computer Data," *Washington Post*, May 27, 1986; and "Are Data Bases a Threat to National Security," *Business Week*, Dec. 1, 1986, p. 39. But DoD officials describe this as "data gathering with no purpose related to immediate actions." (In communications to OTA, May 1987.)

[35]Signed by Walter M. Heiland, Manager, Technology Utilization Office, and addressed to "All TU Officers, IAC Directors and Other Members of the TU Family," and reprinted by *Transnational Data and Communications Report*, February 1987, p. 21.

[36]Letter from Frank C. Carlucci, National Security Advisor, The White House, to the Hon. Jack Brooks, Chairman, Committee on Government Operations, U.S. House of Representatives, Mar. 12, 1987.

[37]Hearings on HR 145 were held on Feb. 26 by the Subcommittee on Legislation and National Security, Committee on Government Operations, U.S. House of Representatives. The White House accepted this measure and the bill was passed by the House in July 1987, and is still waiting to be introduced in the Senate as of early January 1988.

Chapter 6

Constitutional Issues: An Overview

The U.S. Constitution says little about what is a major force in our society: the development and use of science and technology. Yet in spite of its silence about science, the constitutional framework has proved remarkably hospitable to the flowering of scientific research in this century. There has been a strong mutual dependence and respect between government and scientific enterprise that is only rarely threatened. But challenges to the constitutional status of science have occurred in the past, and will surely occur in the future.

The right to free dissemination or communication of scientific research results or other scientific and technical information is not unlimited. It is and has always been limited in the interests of national security.

In spite of its silence about science, the constitutional framework has proved remarkably hospitable to the flowering of scientific research in this century.

Existing restrictions on the flow of scientific information may be administrative, statutory, contractual, or voluntary. The nature of information deemed to be sensitive from the standpoint of national security goes far beyond that related to weapons and includes almost any kind of scientific or technological data that may bear on our industrial capability or competitive position in world trade.[1] National security restrictions on scientific communication apply not only to documents, reports, and publications, but to informal modes of communication, such as talks at professional meetings and participation in scientific seminars. Although primarily applied to information in which government has a "property-type" interest—which results from research carried out by, or contracted out by, government—national security restrictions may also apply in some cases to research done under a government grant for support of basic research, or even, at least in the case of nuclear science and engineering, to information generated entirely without government funding or involvement.

Only a few civil libertarians would disallow any restriction on the dissemination of scientific information, but others believe that the burden created by existing controls is excessive.

Almost all of the people and groups that have spoken out on this issue acknowledge that freedom of speech and press are not absolute and must be balanced against the competing interest of national security. They disagree on where that balance should be struck.

Some people take the middle position that while the current Administration defends a strong position on national security protections and particularly emphasizes the need for strong technology export controls and a dominant role for the military in defining those controls, nevertheless there has been no obvious abuse of authority. The Department of Defense has not pushed dramatically to the theoretical limits of its power to restrict communications.

Others argue that even stronger controls over information are needed to limit the "unwanted transfer" of American science and technology to countries that are very ready to use it against us. The courts have long recognized

[1] Section 1.3 of Executive Order 12356 says that information may be classified "if it concerns military plans, weapons, or operations; the vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security; foreign government information; intelligence activities (including special activities), or intelligence sources or methods; foreign relations or foreign activities of the United States; *scientific, technological, or economic matters relating to the national security;* U.S. Government programs for safeguarding nuclear materials or facilities; cryptology; a confidential source; or other categories of information that are related to the national security . . . ." It also says that such information "shall be classified . . . [when] its unauthorized disclosure, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security." (Emphasis added.)

the need of private parties for protection of their trade secrets. Some urge that a comparable right of protection be granted the government to protect sensitive knowledge generated by government-sponsored research. Thus one can defend a proposition that scientific interchange should, in general, be encouraged; but it is inherently limited by the proprietary nature of scientific knowledge and therefore, unlike political speech, is not protected by the First Amendment.

Critics of this position point out that the information in which government has a property-type interest is exactly the information that should be freely communicated; because government authority to support scientific experimentation flows from its power to spend in order to promote general welfare, and funding that produces that property-interest is generated through taxation of the public.

Only a few civil libertarians would disallow any restriction on the dissemination of scientific information in the interests of national security, but others believe that the burden created by existing controls of several kinds, taken together, is excessive. It has become, they argue, counterproductive in its effects on science and industry, and more importantly, an erosion of constitutional rights and liberties.

There have been only a few direct challenges to the constitutionality of these limitations on the cherished freedom of speech and press. The President as Commander in Chief is considered to have full authority to order classification of government-generated information. Although the constitutionality of some aspects of the Atomic Energy Act and Invention Security Act might be questioned—especially their prior restraint provisions and their applicability to privately generated information—only a few particularly weak challenges have been brought. Ironically, or so it may seem to the layman, restrictions on speech and press under export controls may be less subject to challenge, rather than more so, because their infringement on freedom of speech and press is considered incidental to another legitimate purpose. Yet some critics argue that in this area, the overlapping of national security objectives, rather loosely defined, and economic or industrial objectives, acts to confuse and prejudice the justification of government actions to limit constitutional rights.

Among those who are concerned with preventing the "chilling" effects of excessive restrictions on freedom of speech and press, there is a further difference of opinion. Some argue that science was intended by the Founding Fathers to enjoy a special position and special protection under the First Amendment; and that the courts must recognize and implicitly have recognized that special position. Other scholars deny this special protection and emphasize that the courts have always applied to First Amendment challenges on behalf of scientific communication a "balancing of interests."

Some argue that science was intended by the Founding Fathers to enjoy a special position and special protection under the First Amendment.

Professor Steven Goldberg of The Georgetown University Law Center is among those who argue that science enjoys, under the Constitution, possibly more protection than even political or literary speech. He argues that those who participated in drafting the U.S. Constitution, particularly Jefferson, Madison, Hamilton, and Franklin, were men of the Enlightenment, with broad interests in science, who regarded scientific freedom from constraint by church and state as essential to democracy and constitutionalism.[2] Goldberg argues that the Constitution contains an "implied science clause": that Congress may legislate the establishment of science but not prohibit the free exercise of scientific speech.

[2]Steven Goldberg, "The Constitutional Status of American Science," *University of Illinois Law Forum*, No. 1, 1979, pp. 1-6 ff. Unless otherwise attributed, discussion of Goldberg's views throughout this section is based on this article. Other scholars share the view that scientific communication enjoys an especially protected position under the Constitution. See for example, John A. Robertson, "The Scientist's Right to Research: A Constitutional Analysis," 51 *Southern California Law Review* 1203 (1977); and Delgado & Millen, "God, Galileo, and Government, Toward Constitutional Protection for Scientific Inquiry," 53 *Washington Law Review* 349 (1978).

Under the provisions of Article 1, Section 8, which authorizes Congress to spend money for the general welfare and therefore for scientific research, Goldberg says, "Science is established in the sense that religion cannot be established." The First Amendment was intended to prevent "the suppression of enlightened science by the Church."[3] The "free exercise" and establishment clauses are, Goldberg says, complementary. Science enjoys a protected status.

"A meaningful questioning of the value to the national security of restrictions on scientific expression will, however, come about only if the question is pressed by a vigilant scientific community that will consider and act on these issues creatively and constructively."

He also argues that modern constitutional decisions support this thesis. In *Roth* v. *United States*,[4] concluding that obscenity is outside of First Amendment protection, the Court said that discussion of "sex in scientific works is not itself sufficient reason to deny material the constitutional protection of freedom and press." In *Miller* v. *California*[5] the Court said that the "First Amendment protects works which, taken as a whole, have serious literary, artistic, political, or scientific value." When the Court invalidated an Arkansas statute barring the teaching of evolution in public schools,[6] the Court's scrutiny of the statute (according to Goldberg) "was more intense than in the usual establishment case because the competing value at stake was science."[7]

[3]Goldberg points (p. 5) to Madison's "Memorial and Remonstrance Against Religious Assessments" and to comments on Galileo by Jefferson, saying, "The Jeffersonian wall between church and state was designed in part to protect American Galileos."

[4]354 U.S 476 (1957).

[5]413 U.S. 15 (1973).

[6]*Epperson* v. *Arkansas*, 393 U.S. 97 (1968).

[7]The Court said, "The State's undoubted right to prescribe the curriculum for its public schools does not carry with it the right to prohibit . . . the teaching of a scientific theory or doctrine where that prohibition is based upon reasons that violate the First Amendment." Ibid. at pp. 112-113.

Goldberg maintains that while "The Courts have had little occasion to define precisely the limits of the government's power to classify scientific material," a reading of those decisions that exist and of the opinion of constitutional scholars shows that science "is fully protected by the speech and press clauses." He says:

> As leading first amendment scholars have long recognized, suppression of scientific information is inconsistent with the democratic political process .... Even when scientific work is not immediately applicable to political controversies, it plays an important role in maintaining a free and informed society. Such was the view of the framers, and it has been the consistent view of the courts (p. 16).

Other scholars, such as Professor Harold Green of the National Law Center, discount this thesis. Green says, "There have been Supreme Court and lower court decisions that have involved or have referred to science in protective terms, but the involvement of science in these cases has usually been collateral to some other issue." For example, in the Arkansas case concerned with the teaching of evolution, Green maintains that it was the religious purpose of the statute rather than the restriction on teaching science that was held to violate the First Amendment.

Congress, therefore, has an essential role to play in preserving the balance through the formulation of public policy and the oversight of executive agencies.

Green, like Goldberg, points out that there have been few challenges to the constitutionality of government restrictions on scientific communications. The critical question, he says:

> . . . is the degree of protection that will be afforded against government encroachments in the name of national security, [and] the answer to this question depends on a case by case balancing of the respective interests.
>
> A meaningful questioning of the value to the national security of restrictions on scientific expression will, however, come about only if

> the question is pressed by a vigilant scientific community that will consider and act on these issues creatively and constructively. It is not enough merely to proclaim the shibboleth that science is a sacred preserve entitled, by its very nature, to special constitutional protection.

It may not be adequate for citizens or Congress to rely on scientists to provide the watchful eye and determined protests that will maintain a healthy balancing of interests in safeguarding First Amendment rights. Scientists, after all, are often wrapped up in their immediate scientific pursuits and reluctant to involve themselves in policymaking—at least until their own activities are threatened. Moreover, those scientific pursuits may be entirely dependent on government funding and access to government scientific data.

Congress, therefore, has an essential role to play in preserving the balance through the formulation of public policy and the oversight of executive agencies. The courts nearly always defer to Congress when it presents a consistent, thoughtful position on the constitutional rights of citizens. Moreover, in the absence of congressional action, the executive branch must act. Its daily pressures to assure national security may make it less careful in preserving the essential balance. As Justice Marshall noted in the Pentagon Papers case, unilateral executive efforts to restrain communications without following careful criteria established by Congress may run afoul of the constitutional rule that the executive is not free to legislate.[8]

Gerard Piel, former President of the American Association for the Advancement of Science, argues that there is a social contract embedded in the Constitution through which our society attempts to foster science. Piel points out that Thomas Jefferson, in justifying the First Amendment, argues that "to preserve the freedom of the human mind . . . and freedom of the press" is a cause worthy of martyrdom.[9]

---

[8]See *New York Times Co.* v. *United States*, 403 U.S. 713, 740 (Marshall, J., concurring).

[9]Gerard Piel, "Natural Philosophy in the Constitution," *Science*, vol. 233, No. 5, September 1986, p. 1056.

Appendix

Appendix A

Acknowledgments

Science, Technology, and the Constitution in the Information Age: The Future of the Press and the First Amendment Workshop—Mar. 26, 1987

Vivian Arterbery
Executive Director
U.S. National Commission on Library and Information Science

Joseph Bremner
Database Development, Inc.

Lisa Carlson
Director
Networking Services
Metasystems Design Groups, Inc.

Michael F. Cavanagh
Executive Director
Electronic Mail Association

Mike Greenly
Mike Greenly Consultants

Reed Irvine
Accuracy in Media, Inc.

Richard P. Kleeman
Director
The First Amendment Center

Patrick Maines
President
The Media Institute

Phil Moore
President
Networking & World Information

Richard Neustadt
Private Satellite Network, Inc.

Kendrick Noble, Jr.
Payne Webber, Inc.

David Peyton
Information Industry Association

Monroe Price
Benjamin Cardozo Law School

Judith Roales
Vice President
Independent Newspapers, Inc.

Richard Schmidt, Jr.
Cohn & Marks

Bob Smith
Executive Director
Videotext Industry Association

David Thurm
Counsel
New York Times

Jane Wilson
Assistant Director
Telecommunications Affairs
American Newspaper Publishers Association

Scientific Communications, National Security, and the First Amendment Workshop—Mar. 11, 1987

Allan Adler
American Civil Liberties Union

Kenneth Allen
Information Industry Association

Jerry J. Berman
Director, Project on Privacy and Technology
American Civil Liberties Union

Daniel DeSimone
Executive Director
American Association of Engineering Societies

Diane Fountaine
Director, Information Systems
U.S. Department of Defense

Harlow Freitag
Chairman, Technology Transfer Committee
Institute of Electrical and Electronics Engineers

Stephen Gould
Committee on Scientific Freedom and Responsibility
American Associaton for the Advancement of Science

Harold P. Green
National Law Center
George Washington University

Richard Kleeman
Association of American Publishers

Jonathan Knight
American Association of University Professors

Harold C. Relyea
Specialist in American National Government
Congressional Research Service

Frank Sobieszczyk
Chief, Research Programs Office (DTAG)
U.S. Department of Defense

Paul Stephan
University of Virginia
School of Law

Tom Suttle
Institute of Electrical and Electronic Engineers

Mitchell B. Wallerstein
National Academy of Sciences

Additional Contributors and Reviewers

Part I

Lee Burdick
The Media Institute

Henry Geller
Telecommunications Research and Action Committee

David Littlejohn
University of California, Berkeley

David Peyton
Information Industry Association

David Thurm
New York Times

David Walsh
Electronic Information Services Development

Within OTA:

Richard Dalbello
International Security and Commerce Program

David Margulius
Communications and Information Technologies Program

Mark Nadel
Communications and Information Technologies Program

Part II

Ronald Calinger
The Catholic University

Steven Goldberg
Georgetown University Law Center

Stephen Gould
American Association for the Advancement of Science

Daniel O. Hill
U.S. Department of Commerce

Richard Kleeman
Sigma Delta Chi Foundation

Jonathan Knight
Association of University Professors

Frank Sobieszczyk
U.S. Department of Defense

Mitchell B. Wallerstein
National Academy of Sciences

David Whitman
U.S. Department of Defense

Within OTA:

Richard Dalbello
International Security and Commerce Program

Lisa Heinz
Science, Education and Transportation Program

Nancy Naismith
Science, Education and Transportation Program

Peter Sharfman
International Security and Commerce Program

Chuck Wilk
Communication and Information Technologies Program

U.S. GOVERNMENT PRINTING OFFICE : 1987 - 80-465

Superintendent of Documents Publication Order Form

Order Processing Code
6359

Charge your order. It's easy!

☐ **YES,** please send me the following indicated publications:

Science, Technology, and the First Amendment.
GPO stock number 052-003-01090-9; price $3.50.

1. The total cost of my order is $_____ (International customers please add an additional 25%.) All prices include regular domestic postage and handling and are good through 5/88. After this date, please call Order and Information Desk at 202-783-3238 to verify prices.

Please Type or Print

2. _____
(Company or personal name)

_____
(Additional address/attention line)

_____
(Street address)

_____
(City, State, ZIP Code)

(_____)
(Daytime phone including area code)

3. Please choose method of payment:

☐ Check payable to the Superintendent of Documents
☐ GPO Deposit Account ☐☐☐☐☐☐☐-☐
☐ VISA, CHOICE or MasterCard Account
☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

_____
(Credit card expiration date)

Thank you for your order!

_____
(Signature)

4. Mail To: Superintendent of Documents, Government Printing Office, Washington, D.C. 20402-9325

1/88

Office of Technology Assessment

The Office of Technology Assessment (OTA) was created in 1972 as an analytical arm of Congress. OTA's basic function is to help legislative policymakers anticipate and plan for the consequences of technological changes and to examine the many ways, expected and unexpected, in which technology affects people's lives. The assessment of technology calls for exploration of the physical, biological, economic, social, and political impacts that can result from applications of scientific knowledge. OTA provides Congress with independent and timely information about the potential effects—both beneficial and harmful—of technological applications.

Requests for studies are made by chairmen of standing committees of the House of Representatives or Senate; by the Technology Assessment Board, the governing body of OTA; or by the Director of OTA in consultation with the Board.

The Technology Assessment Board is composed of six members of the House, six members of the Senate, and the OTA Director, who is a non-voting member.

OTA has studies under way in nine program areas: energy and materials; industry, technology, and employment; international security and commerce; biological applications; food and renewable resources; health; communication and information technologies; oceans and environment; and science, education, and transportation.

CONGRESS OF THE UNITED STATES
OFFICE OF TECHNOLOGY ASSESSMENT
WASHINGTON, D.C. 20510-8025

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

POSTAGE AND FEES PAID
OFFICE OF TECHNOLOGY ASSESSMENT

379

OTA-CIT-369

JANUARY 1988